Combinatorics, Probability and Computing (2021), **30**, pp. 930–941
doi:10.1017/S0963548321000109

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Additive bases via Fourier analysis

Bodan Arsovski

Skopje, North Macedonia
Email: bodan.arsovski@outlook.com

(Received 27 February 2020; revised 9 November 2020; accepted 12 November 2020; first published online 29 April 2021)

Abstract

Extending a result by Alon, Linial, and Meshulam to abelian groups, we prove that if G is a finite abelian group of exponent m and S is a sequence of elements of G such that any subsequence of S consisting of at least $|S| - m \ln |G|$ elements generates G, then S is an additive basis of G. We also prove that the additive span of any l generating sets of G contains a coset of a subgroup of size at least $|G|^{1-c\epsilon^l}$ for certain $c = c(m)$ and $\epsilon = \epsilon(m) < 1$; we use the probabilistic method to give sharper values of $c(m)$ and $\epsilon(m)$ in the case when G is a vector space; and we give new proofs of related known results.

2020 MSC Codes: Primary 11P99; Secondary 05E99

1. Introduction

Alon, Linial, and Meshulam [1] prove three theorems which roughly say that a 'sufficiently linearly independent' set of vectors in a finite-dimensional vector space over $\mathbb{F}_p$ additively spans the space. These results are motivated by the study of flows in graphs, and in particular the conjecture made by Jaeger, Linial, Payan, and Tarsi [3]. The first of the three theorems has been generalized to finite abelian groups by Lev, Muzychuk, and Pinchasi [4] via the Ruzsa sum triangle inequality, and Hatami and de Quehen [2] via the Plünnecke–Ruzsa inequality. In this article, we extend the other two theorems in [1] to finite abelian groups, though we note that in the case when G is a vector space the bounds obtained by Alon, Linial, and Meshulam are slightly stronger than the ones obtained here. Along the way we also prove that if G is a finite abelian group of exponent m and $B_1, \dots, B_l$ are generating sets of G, then the additive span of the multiset union $\uplus_{i=1}^{l} B_i$ contains a coset of a subgroup $H \leqslant G$ which has size

$$|H| \geqslant |G|^{1-c(m)\epsilon(m)^l}, \tag{1.1}$$

for $c(m) = m \ln m + 1$ and

$$\epsilon(m) = \frac{\ln m}{2 \ln m - \ln (m-1)} \leqslant \frac{m \ln m}{m \ln m + 1} < 1. \tag{1.2}$$

In the case when G is a vector space, we use the probabilistic method to give sharper values of $c(m)$ and $\epsilon(m)$. To be more precise, we prove that if p is a prime number, l and n are positive integers,

© The Author(s), 2021. Published by Cambridge University Press.

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

and V is an n-dimensional vector space over $\mathbb{F}_p$, then the additive span of any l linear bases of V contains an affine subspace of dimension at least

$$n\left(1-(p-1)^2\left(\frac{p-2}{p-1}\right)^{l-1}\right). \tag{1.3}$$

We also obtain new proofs of related known results.

1.1 Notation

Let G be a finite abelian group of exponent m. For a sequence $S=(g_1,\dots,g_l)$ of elements of G, let $|S|=l$ be the length of S. Let G^* be the dual group of characters $G\to\mathbb{C}$. There is the isomorphism $G\cong G^{**}$ given by identifying $g\in G$ with the character $G^*\to\mathbb{C}$ that maps $\varphi\in G^*\mapsto\varphi(g)$. We write $g(\varphi)=\varphi(g)$ for $g\in G$ and $\varphi\in G^*$. For $g\in G$, we define $g^\circ\leqslant G^*$ as the annihilator of g—the subgroup consisting of those $\varphi\in G^*$ such that $\varphi(g)=1$. For a subgroup $H\leqslant G$, we define $H^\circ=\cap_{h\in H}h^\circ$, and for $\varphi\in G^*$ and $L\leqslant G^*$ we similarly define the annihilators $\varphi^\circ\leqslant G$ and $L^\circ\leqslant G$. For $g\in G$, we define $\langle g\rangle$ as the subgroup of G generated by g, and for a subset $X\leqslant G$ (or a multiset X consisting of elements of G) we define $\langle X\rangle$ as the subgroup of G generated by X. For a map $f:G\to\mathbb{C}$, we define its Fourier transform $\widehat{f}:G^*\to\mathbb{C}$ by the equation

$$\widehat{f}(\varphi)=\sum_{g\in G}\varphi(g)f(g)\text{ for }\varphi\in G^*. \tag{1.4}$$

In this notation, the Fourier inversion formula is

$$f(g)=|G|^{-1}\sum_{\varphi\in G^*}\varphi(-g)\widehat{f}(\varphi)\text{ for }g\in G, \tag{1.5}$$

and the uncertainty principle is

$$|\operatorname{supp}f|\cdot|\operatorname{supp}\widehat{f}|\geqslant|G|. \tag{1.6}$$

Here $\operatorname{supp}f$ denotes the set of $g\in G$ such that $f(g)\neq0$, and $\operatorname{supp}\widehat{f}$ denotes the set of $\varphi\in G^*$ such that $\widehat{f}(\varphi)\neq0$. Equations (1.5) and (1.6) are standard results in Fourier analysis (see, e.g., [5]), so we omit their proofs. We define the additive span of a sequence $(g_1,\dots,g_l)$ of elements of G as

$$\operatorname{addspan}(g_1,\dots,g_l)=\left\{g\in G\,|\,g=\epsilon_1g_1+\cdots+\epsilon_lg_l\text{ for some }\epsilon_1,\dots,\epsilon_l\in\{0,1\}\right\}, \tag{1.7}$$

and we similarly define the additive span of a (multi)set. We say that a sequence (or a (multi)set) is an additive basis of G if its additive span is G. Let $\alpha(G)$ be the smallest positive integer with the property that the multiset union of any $\alpha(G)$ generating sets of G is an additive basis of G.

1.2 Main results

First we prove the following two general theorems.

Theorem 1.1. *Let $(g_1,\dots,g_l)$ be a sequence of elements of G and let $\varphi_1,\dots,\varphi_l\in G^*$ be such that*

$$P=G^*\setminus\left(\cup_{i=1}^l(\varphi_i+g_i^\circ)\right), \tag{1.8}$$

is non-empty.

1. *If P is contained in a coset of a subgroup $H\leqslant G^*$, then the additive span of $(g_1,\dots,g_l)$ contains a coset of $H^\circ\leqslant G$.*

2. *The additive span of $(g_1,\dots,g_l)$ has at least $|P|^{-1}|G|$ elements.*

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

Here $\varphi_i + g_i^\circ$ is a coset of $g_i^\circ \leqslant G^*$ for $i \in \{1, \dots, l\}$. Put in other words, part (1.1) of Theorem 1.1 says that if we can find cosets of $g_1^\circ, \dots, g_l^\circ$ whose union covers most of G^* in a way that (*a*) uncovered points exist, and (*b*) all uncovered points belong to a coset of $H \leqslant G^*$, then the additive span of $(g_1, \dots, g_l)$ contains a coset of $H^\circ \leqslant G$.

Theorem 1.2. *Let $S = (g_1, \dots, g_l)$ be a sequence of elements of G, and let $P \neq \varnothing$ be a non-empty subset of G^*. Then there is a subsequence $S' = (g_1', \dots, g_{l'}')$ of S and elements $\varphi_1, \dots, \varphi_{l'} \in G^*$ such that the set*

$$P' = P \setminus \left(\cup_{i=1}^{l'} (\varphi_i + g_i'^{\circ})\right), \tag{1.9}$$

is contained in a coset of $\langle S \backslash S' \rangle^\circ$ and has size

$$1 \leqslant |P'| \leqslant \left(1 - \frac{1}{m}\right)^{l'} |P|. \tag{1.10}$$

Here $S \backslash S'$ is perhaps a slight abuse of notation, so let us explain what it means exactly. We think of a subsequence of S as selecting some indices and discarding the others, and we use $S \backslash S'$ to denote the subsequence of S consisting of precisely those indices that are *not* selected for S'.

The main results in this article are the following two corollaries of Theorems 1.1 and 1.2, which are analogues of Propositions 4.1 and 4.2 in [1] in the general case of finite abelian groups.

Corollary 1.3. *Let S be a sequence of elements of G such that any subsequence of S consisting of at least $|S| - m \ln |G|$ elements generates G. Then S is an additive basis of G. In fact, S contains a subsequence consisting of at most $m \ln |G|$ elements which is an additive basis of G.*

Corollary 1.4. *Let $B_1, \dots, B_l$ be generating sets of G. If*

$$l \geqslant (m \ln m + 1)(\ln \ln |G| + 1), \tag{1.11}$$

then there are subsets $A_1 \subseteq B_1, \dots, A_l \subseteq B_l$ such that $\sum_{i=1}^{l} |A_i| \leqslant m \ln |G|$ and $\uplus_{i=1}^{l} A_i$ (the multiset union) is an additive basis of G.

In fact, we can show the following stronger version of Corollary 1.3.

Corollary 1.3'. *Let S be a sequence of elements of G. Then S has a subsequence S' consisting of at most $m \ln |G|$ elements such that the additive span of S' contains a coset of $\langle S \backslash S' \rangle$.*

We also show the following corollary, which is a generalization of Corollary 1.3'.

Corollary 1.5. *Let $B_1, \dots, B_l$ be generating sets of G, and let S be a sequence of elements of G. Let B be the multiset of elements of S. Let*

$$\epsilon = \epsilon(m) = \frac{\ln m}{2 \ln m - \ln (m-1)} \leqslant \frac{m \ln m}{m \ln m + 1} < 1. \tag{1.12}$$

Then S has a subsequence S' consisting of at most $m \ln |G| \, \epsilon^l$ elements such that the additive span of the multiset union $B' \uplus \left(\uplus_{i=1}^{l} B_i\right)$ contains a coset of $\langle S \backslash S' \rangle$, where B' is the multiset of elements of S'.

As a consequence, we deduce the following corollary.

Corollary 1.6. *Let $B_1, \dots, B_l$ be generating sets of G. Let*

$$c = c(m) = m \ln m + 1, \tag{1.13}$$

and let $\epsilon = \epsilon(m)$ be as in Corollary 1.5. Then the additive span of the multiset union $\uplus_{i=1}^{l} B_i$ contains a coset of a subgroup $H \leqslant G$ which has size

$$|H| \geqslant |G|^{1 - c\epsilon^l}. \tag{1.14}$$

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

By using the probabilistic method, we can deduce two more corollaries of Theorem 1.1. For $s \in G$ and $\phi \in G^*$ let

$$\eta_G(s,\phi) = \begin{cases} 1 - \frac{1}{[G^* : s^\circ]-1} & \text{if } \phi \notin s^\circ, \\ 1 & \text{if } \phi \in s^\circ, \end{cases} \tag{1.15}$$

where $[G^* : s^\circ]$ is the index of the subgroup $s^\circ \leqslant G^*$, and for $l \in \mathbb{Z}_{\geqslant 0}$ let

$$\mathbf{M}_G(l) = \left\lfloor \max \left\{ \sum_{\phi \in G^*} \prod_{b \in B} \eta_G(b,\phi)^l \;\middle|\; B \text{ is a generating set of } G \right\} \right\rfloor. \tag{1.16}$$

Corollary 1.7. *Let S be a sequence of elements of G. Then*

$$\left|\text{addspan } S\right| \geqslant \left\lfloor \sum_{\phi \in G^*} \prod_{s \in S} \eta_G(s,\phi) \right\rfloor^{-1} |G|. \tag{1.17}$$

Corollary 1.8. *Let $B_1, \ldots, B_l$ be generating sets of G. Then*

$$\left|\text{addspan } (\uplus_{i=1}^l B_i)\right| \geqslant \mathbf{M}_G(l)^{-1} |G|. \tag{1.18}$$

1.3 Relation to known results

Corollary 1.4 implies the main results of [4] and [2] with a weaker leading term. To be precise, a consequence of Corollary 1.4 is that

$$\alpha(G) \leqslant \lceil (m \ln m + 1)(\ln \ln |G| + 1) \rceil, \tag{1.19}$$

while in [4] and [2] it is shown that $\alpha(G) \leqslant \lceil 2m \ln \log_2 |G| \rceil$. We suspect that the smallest l such that $\mathbf{M}_G(l)$ is equal to 1 is smaller than $(m \ln m + 1)(\ln \ln |G| + 1)$, and so Corollary 1.8 gives a better upper bound for $\alpha(G)$ than Corollary 1.4. However, computing $\mathbf{M}_G(l)$ seems to be difficult for general groups G. When p is a prime number and $G = V$ is an n-dimensional vector space over $\mathbb{F}_p$,

$$\mathbf{M}_V(l) = \left\lfloor \left(1 + (p-1)\left(\frac{p-2}{p-1}\right)^l\right)^n \right\rfloor. \tag{1.20}$$

So Corollary 1.8 implies the following result.

Corollary 1.9. *Let p be a prime number and n be a positive integer, let V be an n-dimensional vector space over $\mathbb{F}_p$, and let $B_1, \ldots, B_l$ be linear bases of V.*

(1) We have

$$\left|\text{addspan } (\uplus_{i=1}^l B_i)\right| \geqslant \left\lfloor \left(1 + (p-1)\left(\frac{p-2}{p-1}\right)^l\right)^n \right\rfloor^{-1} p^n \geqslant p^{n\left(1 - \frac{p-1}{\ln p}\left(\frac{p-2}{p-1}\right)^l\right)}. \tag{1.21}$$

(2) In fact, the additive span of $\uplus_{i=1}^l B_i$ contains an affine subspace of dimension at least

$$n\left(1 - (p-1)^2\left(\frac{p-2}{p-1}\right)^{l-1}\right). \tag{1.22}$$

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

(3) In particular,

$$\alpha(V) \leqslant \left\lceil \frac{\ln n + \ln(p-1) - \ln\ln 2}{\ln(p-1) - \ln(p-2)} \right\rceil. \tag{1.23}$$

Parts (1) and (3) of Corollary 1.9 are known in slightly sharper forms (see proposition 3.1 in [1] and section 2 of [4]), and part (2) of Corollary 1.9 is new.

2. Proofs

2.1 Proofs of Theorems 1.1 and 1.2

In this subsection, we prove Theorems 1.1 and 1.2. The main idea consists of finding a function whose support is contained in the additive span of the given sequence, and showing that this support contains a coset of the given subgroup by analysing the Fourier transform.

Proof of Theorem 1.1. Let us first prove part (1.1) of the theorem. Let $S = (g_1, \dots, g_l)$, and let $f_S : G \to \mathbb{C}$ be the map defined by

$$f_S(g) = \sum_{\substack{\epsilon_1,\dots,\epsilon_l \in \{0,1\} \\ \epsilon_1 g_1 + \cdots + \epsilon_l g_l = g}} (-1)^{\epsilon_1+\cdots+\epsilon_l} \prod_{i=1}^{l} \varphi_i(g_i)^{-1} \text{ for } g \in G. \tag{2.1}$$

For $i \in \{1, \dots, l\}$, recall that we have

$$g_i(\varphi - \varphi_i) = (\varphi - \varphi_i)(g_i) = \varphi(g_i)\varphi_i(g_i)^{-1}, \tag{2.2}$$

and so

$$\begin{aligned}
&\prod_{i=1}^{l} (1 - g_i(\varphi - \varphi_i)) \\
&\quad = \sum_{\epsilon_1,\dots,\epsilon_l \in \{0,1\}} (-1)^{\epsilon_1+\cdots+\epsilon_l} \varphi(g_1 + \cdots + g_l) \prod_{i=1}^{l} \varphi_i(g_i)^{-1} \\
&\quad = \sum_{g \in G} \left(\sum_{\substack{\epsilon_1,\dots,\epsilon_l \in \{0,1\} \\ \epsilon_1 g_1 + \cdots + \epsilon_l g_l = g}} (-1)^{\epsilon_1+\cdots+\epsilon_l} \varphi(g) \prod_{i=1}^{l} \varphi_i(g_i)^{-1} \right) \\
&\quad = \sum_{g \in G} \varphi(g) f_S(g).
\end{aligned} \tag{2.3}$$

Equations (1.4) and (2.3) imply that the Fourier transform $\widehat{f_S} : G^* \to \mathbb{C}$ of f_S satisfies the equation

$$\widehat{f_S}(\varphi) = \prod_{i=1}^{l} (1 - g_i(\varphi - \varphi_i)) \text{ for } \varphi \in G^*. \tag{2.4}$$

If $\varphi \in \varphi_i + g_i^\circ$ for some $i \in \{1, \dots, l\}$, then

$$(\varphi - \varphi_i)(g_i) = 1 \Longrightarrow 1 - g_i(\varphi - \varphi_i) = 0 \Longrightarrow \widehat{f_S}(\varphi) = 0. \tag{2.5}$$

Conversely, if $\varphi \notin \cup_{i=1}^{l} (\varphi_i + g_i^\circ)$ then, for all $i \in \{1, \dots, l\}$, $1 - g_i(\varphi - \varphi_i) \neq 0$, implying that $\widehat{f_S} \neq 0$. So the support of $\widehat{f_S}$ is exactly equal to $G^* \setminus \left(\cup_{i=1}^{l} (\varphi_i + g_i^\circ) \right)$, i.e.,

$$\operatorname{supp} \widehat{f_S} = G^* \setminus \left(\cup_{i=1}^{l} (\varphi_i + g_i^\circ) \right) = P. \tag{2.6}$$

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

Since P is non-empty by assumption, $\widehat{f_S}$ is not identically zero, and since P is contained in $\psi + H$ by assumption, equation (1.4) implies that

$$\begin{aligned} f_S(g) &= |G|^{-1} \sum_{\varphi \in G^*} \varphi(-g)\widehat{f_S}(\varphi) \\ &= |G|^{-1} \sum_{\varphi \in \operatorname{supp} \widehat{f_S}} \varphi(-g)\widehat{f_S}(\varphi) \\ &= |G|^{-1} \sum_{\varphi \in \psi + H} \varphi(-g)\widehat{f_S}(\varphi) \\ &= \psi(g)^{-1} |G|^{-1} \sum_{\phi \in H} \phi(-g)\widehat{f_S}(\psi + \phi). \end{aligned} \tag{2.7}$$

The second equality is true because $\widehat{f_S}(\varphi) = 0$ for $\varphi \notin \operatorname{supp} \widehat{f_S}$, the third equality is true because $\operatorname{supp} \widehat{f_S} \subseteq \psi + H$, and the fourth equality is a change of the variable φ to $\phi = \varphi - \psi$. If $g_1 - g_2 \in H^\circ$, then $\phi(-g_1) = \phi(-g_2)$ for all $\phi \in H$, so equation (2.7) implies that

$$\begin{aligned} \psi(g_1) f_S(g_1) &= |G|^{-1} \sum_{\phi \in H} \phi(-g_1)\widehat{f_S}(\psi + \phi) \\ &= |G|^{-1} \sum_{\phi \in H} \phi(-g_2)\widehat{f_S}(\psi + \phi) = \psi(g_2) f_S(g_2). \end{aligned} \tag{2.8}$$

Since $\widehat{f_S}$ is not identically zero, f_S is not identically zero, so there is an element $g \in G$ such that $f_S(g) \neq 0$. Equation (2.8) implies that

$$f_S(g + h) = \psi(h)^{-1} f_S(g) \neq 0 \text{ for } h \in H^\circ, \tag{2.9}$$

and by equation (2.1) that in particular means that

$$\{(\epsilon_1, \ldots, \epsilon_l) \mid \epsilon_1, \ldots, \epsilon_l \in \{0, 1\} \,\&\, \epsilon_1 g_1 + \cdots + \epsilon_l g_l = g + h\} \neq \varnothing \text{ for } h \in H^\circ, \tag{2.10}$$

i.e., that $g + h \in \operatorname{addspan}(g_1, \ldots, g_l)$ for all $h \in H^\circ$, which is what we wanted to prove.

Now let us prove part (1.1) of the theorem. As in the proof of part (1.1), we have a function $f_S : G \to \mathbb{C}$ such that $\operatorname{supp} f_S \subseteq \operatorname{addspan} S$ and $\operatorname{supp} \widehat{f_S} = P$. Then equation (1.6) implies that

$$\left|\operatorname{addspan} S\right| \geqslant \left|\operatorname{supp} f_S\right| \geqslant \left|\operatorname{supp} \widehat{f_S}\right|^{-1} |G| = |P|^{-1} |G|, \tag{2.11}$$

and that completes the proof. □

Proof of Theorem 1.2. We choose elements $\phi_1, \ldots, \phi_l \in G^*$ one-by-one as follows. Once $\phi_1, \ldots, \phi_{t-1}$ have been chosen for $t \in \{1, \ldots, l\}$, we choose ϕ_t in a way that minimizes the set size $\left|P \setminus \left(\cup_{i=1}^t (\phi_i + g_i^\circ)\right)\right|$ but keeps it positive; if there are multiple such choices for ϕ_t, then we pick one randomly. There are two possibilities for each $t \in \{1, \ldots, l\}$:

(1) $\left|P \setminus \left(\cup_{i=1}^t (\phi_i + g_i^\circ)\right)\right| = \left|P \setminus \left(\cup_{i=1}^{t-1} (\phi_i + g_i^\circ)\right)\right|$. If we pick

$$\phi \in P \setminus \left(\cup_{i=1}^{t-1} (\phi_i + g_i^\circ)\right) \neq \varnothing, \tag{2.12}$$

and pick $\phi_t' \in \phi - g_t^\circ$, then

$$\left|P \setminus \left((\phi_t' + g_t^\circ) \cup_{i=1}^{t-1} (\phi_i + g_i^\circ)\right)\right| < \left|P \setminus \left(\cup_{i=1}^{t-1} (\phi_i + g_i^\circ)\right)\right|, \tag{2.13}$$

which, since ϕ_t is chosen optimally, must mean that

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

$$\left|P \setminus \left((\phi_t' + g_t^\circ) \cup_{i=1}^{t-1} (\phi_i + g_i^\circ)\right)\right| = 0 \implies \phi_t' + g_t^\circ \supseteq P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right). \tag{2.14}$$

In this case, we do not select the entry indexed t for the subsequence S'.

(2) $\left|P \setminus \left(\cup_{i=1}^{t}(\phi_i + g_i^\circ)\right)\right| < \left|P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right)\right|$. Note that

$$\frac{|G|}{m} \mid \frac{|G|}{|\langle g_t \rangle|} = |g_t^\circ|. \tag{2.15}$$

So g_t° has at most m cosets, and they cover G^*. Therefore, some coset covers at least $\frac{1}{m}$ of the points of $P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right)$. Moreover, there is no coset of g_t° that contains all of the points of $P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right)$, since if there was then $\left|P \setminus \left(\cup_{i=1}^{t}(\phi_i + g_i^\circ)\right)\right| > 0$ would imply that $\left|P \setminus \left(\cup_{i=1}^{t}(\phi_i + g_i^\circ)\right)\right| = \left|P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right)\right|$ and we would be in the first case. Since ϕ_t is chosen optimally, we must have

$$\left|P \setminus \left(\cup_{i=1}^{t}(\phi_i + g_i^\circ)\right)\right| \leqslant \left(1 - \frac{1}{m}\right) \left|P \setminus \left(\cup_{i=1}^{t-1}(\phi_i + g_i^\circ)\right)\right|. \tag{2.16}$$

In this case, we select the entry indexed t for the subsequence S'.

Because of the way we choose $\phi_1, \ldots, \phi_l$, we have

$$P \setminus \left(\cup_{i=1}^{l}(\phi_i + g_i^\circ)\right) = P \setminus \left(\cup_{i=1}^{l'}(\varphi_i + g_i'^\circ)\right) = P', \tag{2.17}$$

where $(\varphi_1, \ldots, \varphi_{l'})$ is the subsequence of $(\phi_1, \ldots, \phi_l)$ corresponding to the subsequence S' of S. Since $P' \neq \varnothing$, because of the way we choose $\phi_1, \ldots, \phi_l$ we must have

$$1 \leqslant \left|P'\right| = \left|P \setminus \left(\cup_{i=1}^{l}(\phi_i + g_i^\circ)\right)\right| \leqslant \left(1 - \frac{1}{m}\right)^{|S'|} |P|, \tag{2.18}$$

and if $t \in \mathbb{Z}$ is such that the tth entry of S is not selected for the subsequence S', then there is an element $\phi_t' \in G^*$ such that

$$P' = P \setminus \left(\cup_{i=1}^{l}(\phi_i + g_i^\circ)\right) \subseteq \phi_t' + g_t^\circ. \tag{2.19}$$

It follows that P' is contained in a coset of g_t° for all $t \in \mathbb{Z}$ such that the tth entry of S is not selected for S'. This in turn implies that P' is contained in a coset of $\langle S \setminus S' \rangle^\circ$. □

2.2 Proofs of Corollaries 1.3, 1.3', 1.4, 1.5, and 1.6

In this subsection, we prove Corollaries 1.3, 1.3', 1.4, 1.5, and 1.6. We deduce Corollaries 1.3', 1.4, and 1.5 from Theorems 1.1 and 1.2. Then we note that Corollary 1.3 is an immediate consequence of Corollary 1.3', and we deduce Corollary 1.6 from Corollary 1.5.

Proof of Corollary 1.3'. Let us denote $S = (g_1, \ldots, g_l)$. By Theorem 1.2 applied to S and the set $P = G^*$, there is a subsequence $S' = (g_1', \ldots, g_{l'}')$ of S and elements $\varphi_1, \ldots, \varphi_{l'} \in G^*$ such that the set

$$P' = G^* \setminus \left(\cup_{i=1}^{l'}(\varphi_i + g_i'^\circ)\right), \tag{2.20}$$

is contained in a coset of $\langle S \setminus S' \rangle^\circ$ and has size

$$1 \leqslant \left|P'\right| \leqslant \left(1 - \frac{1}{m}\right)^{|S'|} \left|G^*\right| = \left(1 - \frac{1}{m}\right)^{|S'|} |G|. \tag{2.21}$$

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

Equation (2.21) implies that

$$|S'| \ln \frac{m}{m-1} \leqslant \ln |G| \implies |S'| \leqslant m \ln |G| \,. \tag{2.22}$$

Part (1.1) of Theorem 1.1 then implies that the additive span of S' contains a coset of $\langle S \backslash S' \rangle$. □

Corollary 1.3 is an immediate consequence of Corollary 1.3'—we omit the details.

Proof of Corollary 1.4. Let $S_1, \ldots, S_l$ be sequences such that $|S_i| = |B_i|$ and the set of elements of S_i is B_i, for $i \in \{1, \ldots, l\}$. By Theorem 1.2, there exist subsequences $S'_1, \ldots, S'_l$ of $S_1, \ldots, S_l$, and elements $\varphi(i,s), \psi_i \in G^*$ for $i \in \{1, \ldots, l\}$ and $s \in S'_i$, such that the sets $P_0, \ldots, P_l$ defined by $P_0 = G^*$ and

$$P_i = P_{i-1} \setminus \left(\cup_{s \in S'_i} (\varphi(i,s) + s^\circ) \right) \text{ for } i \in \{1, \ldots, l\}, \tag{2.23}$$

satisfy

$$P_i \subseteq \psi_i + \langle S_i \backslash S'_i \rangle^\circ \text{ and } 1 \leqslant |P_i| \leqslant \left(1 - \frac{1}{m}\right)^{|S'_i|} |P_{i-1}| \text{ for } i \in \{1, \ldots, l\}. \tag{2.24}$$

Note that the inductive definition of $P_0, \ldots, P_l$ implies that

$$P_i = G^* \setminus \left(\cup_{j=1}^{i} \cup_{s \in S'_j} (\varphi(j,s) + s^\circ) \right) \text{ for } i \in \{1, \ldots, l\}. \tag{2.25}$$

Let S be the concatenation of $S_1, \ldots, S_l$, so that the multiset of elements of S is $\uplus_{i=1}^{l} B_i$. Let S' be the subsequence of S consisting of those entries that are selected for the subsequences $S'_1, \ldots, S'_l$. The fact that

$$1 \leqslant |P_l| \leqslant \left(1 - \frac{1}{m}\right)^{|S'_1| + \cdots + |S'_l|} \left|G^*\right| = \left(1 - \frac{1}{m}\right)^{|S'|} |G| \,, \tag{2.26}$$

implies that

$$|S'| \ln \frac{m}{m-1} \leqslant \ln |G| \implies |S'| \leqslant m \ln |G| \,. \tag{2.27}$$

For $i \in \{1, \ldots, l\}$, let A_i be the set of elements of S'_i, so that the set of elements of S' is $\uplus_{i=1}^{l} A_i$ and we have $\sum_{i=1}^{l} |A_i| \leqslant m \ln |G|$. We want to show that S' is an additive basis of G. First let us note that, for $i \in \{1, \ldots, l\}$, the subgroup $\langle S_i \backslash S'_i \rangle$ has at least $m^{-|S'_i|} |G|$ elements (since adding the elements of S'_i to it results in a generating set of G), and therefore $\langle S_i \backslash S'_i \rangle^\circ$ has at most $m^{|S'_i|}$ elements. Since P_i is contained in a coset of $\langle S_i \backslash S'_i \rangle^\circ$ for $i \in \{1, \ldots, l\}$, we have

$$|P_i| \leqslant m^{|S'_i|} \text{ for } i \in \{1, \ldots, l\}. \tag{2.28}$$

Equations (2.24) and (2.28) imply that

$$|P_i| \leqslant \min \left\{ \left(1 - \frac{1}{m}\right)^{|S'_i|} |P_{i-1}| \,, m^{|S'_i|} \right\} \text{ for } i \in \{1, \ldots, l\}. \tag{2.29}$$

Let

$$0 < \epsilon = \frac{\ln m}{2 \ln m - \ln (m-1)} < 1. \tag{2.30}$$

Then equation (2.29) implies that

$$|P_i| \leqslant \left(\left(1 - \frac{1}{m}\right)^{|S'_i|} |P_{i-1}| \right)^{\epsilon} m^{(1-\epsilon)|S'_i|} = |P_{i-1}|^{\epsilon} \text{ for } i \in \{1, \ldots, l\}, \tag{2.31}$$

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

which by induction implies that

$$|P_i| \leqslant |G|^{\epsilon^i} \text{ for } i \in \{1, \dots, l\}. \tag{2.32}$$

Therefore

$$\ln |P_l| \leqslant \epsilon^l \ln |G| \leqslant e^{\ln \epsilon (m \ln m + 1)(\ln \ln |G| + 1)} \ln |G| \leqslant e^{-(\ln \ln |G| + 1)} \ln |G| = e^{-1}, \tag{2.33}$$

implying that $|P_l| \leqslant e^{e^{-1}} < 1.5$. Since P_l is non-empty, it follows that $|P_l| = 1$. Then equation (2.23) implies that the union of the cosets $\varphi(i, s) + s^\circ$ for $i \in \{1, \dots, l\}$ and $s \in S'_i$ is equal to G^* minus a single point, which by (either part of) Theorem 1.1 implies that S' is indeed an additive basis of G.

□

Proof of Corollary 1.5. As in the proof of Corollary 1.4, we can find cosets of b° for $b \in \uplus_{i=1}^l B_i$ such that the complement P_l of the union of these cosets satisfies

$$1 \leqslant |P_l| \leqslant |G|^{\epsilon^l}. \tag{2.34}$$

Suppose that $S = (b_1, \dots, b_w)$. By Theorem 1.2 applied to the sequence S and the set $P = P_l$, we can find a subsequence $S' = (b'_1, \dots, b'_{w'})$ of S and cosets $C(b'_1), \dots, C(b'_{w'})$ of $(b'_1)^\circ, \dots, (b'_{w'})^\circ$ such that the set

$$P' = P_l \setminus \left(\cup_{j=1}^{w'} C(b'_j) \right), \tag{2.35}$$

is contained in a coset of $\langle S \backslash S' \rangle^\circ$ and has size

$$1 \leqslant |P'| \leqslant \left(1 - \frac{1}{m}\right)^{w'} |P_l| \leqslant \left(1 - \frac{1}{m}\right)^{w'} |G|^{\epsilon^l}. \tag{2.36}$$

Equation (2.36) and the fact that $1 + z \leqslant e^z$ for all $z \in \mathbb{R}$ imply that

$$w' \leqslant m \ln |G| \, \epsilon^l. \tag{2.37}$$

So if B' is the multiset of elements of S', then we can find cosets of b° for $b \in B' \uplus (\uplus_{i=1}^l B_i)$ such that the complement of the union of these cosets is non-empty and contained in a coset of $\langle S \backslash S' \rangle^\circ$, and part (1.1) of Theorem 1.1 then implies that the additive span of $B' \uplus (\uplus_{i=1}^l B_i)$ contains a coset of $H = \langle S \backslash S' \rangle \leqslant G$. □

Proof of Corollary 1.6. If $l = 0$, then the claim is evident, so let us suppose that $l \geqslant 1$. Then Corollary 1.5 implies that B_l has a subset B' consisting of at most $m \ln |G| \, \epsilon^{l-1}$ elements such that the additive span of the multiset union

$$B_l \uplus \left(\uplus_{i=1}^{l-1} B_i \right) = \uplus_{i=1}^l B_i, \tag{2.38}$$

contains a coset of $H = \langle B_l \backslash B' \rangle$. Since adding $|B'|$ elements (each of order at most m) to H results in a generating set of G, we have

$$|H| \geqslant m^{-|B'|} |G|. \tag{2.39}$$

The lower bound for $|H|$ follows from

$$m^{-|B'|} |G| \geqslant m^{-m \ln |G| \epsilon^{l-1}} |G| = |G|^{1 - (m \ln m) \epsilon^{l-1}} \geqslant |G|^{1 - c\epsilon^l}. \tag{2.40}$$

□

2.3 Proofs of Corollaries 1.7, 1.8, and 1.9

In this subsection, we use the probabilistic method to prove Corollary 1.7, and then we deduce Corollaries 1.8 and 1.9 as special cases.

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

Proof of Corollary 1.7. Without loss of generality, we may assume that S does not contain the identity. For each $s \in S$, let us select a coset $C(s)$ of s° that does not contain the identity (and is therefore distinct from s°) uniformly and at random. For $\phi \in G^*$, let X_ϕ be the random variable which takes the value 1 if ϕ does not belong to any of the selected cosets and takes the value 0 otherwise. For example, since none of the cosets contain the identity id_{G^*} of G^*, $X_{\mathrm{id}_{G^*}}$ always takes the value 1. We have

$$\mathbb{E}\left(X_\phi\right) = \prod_{s\in S} \mathbb{P}\left(\phi \notin C(s)\right) = \prod_{s\in S} \eta_G(s,\phi) \text{ for } \phi \in G^*. \tag{2.41}$$

Therefore,

$$\mathbb{E}\left(\sum_{\phi\in G^*} X_\phi\right) = \sum_{\phi\in G^*}\prod_{s\in S} \eta_G(s,\phi), \tag{2.42}$$

implying, by Markov's inequality, that

$$\mathbb{P}\left(\sum_{\phi\in G^*} X_\phi \leqslant \left\lfloor \sum_{\phi\in G^*}\prod_{s\in S} \eta_s(\phi)\right\rfloor\right) \geqslant 1 - \frac{\mathbb{E}\left(\sum_{\phi\in G^*} X_\phi\right)}{1+\left\lfloor \sum_{\phi\in G^*}\prod_{s\in S} \eta_s(\phi)\right\rfloor} > 0. \tag{2.43}$$

So there is a selection of cosets $C(s)$ such that the complement of the union of the cosets contains the identity of G^* and has at most

$$\left\lfloor \sum_{\phi\in G^*}\prod_{s\in S} \eta_s(\phi)\right\rfloor, \tag{2.44}$$

points. Then part (1.1) of Theorem 1.1 completes the proof. □

Proof of Corollary 1.8. Corollary 1.7 implies that

$$\left|\uplus_{i=1}^{l} B_i\right| \geqslant \left\lfloor \sum_{\phi\in G^*}\prod_{i=1}^{l}\prod_{b\in B_i} \eta_G(b,\phi)\right\rfloor^{-1} |G|\,. \tag{2.45}$$

The inequality between the arithmetic mean and the geometric mean of a list of positive numbers implies that

$$\left\lfloor \sum_{\phi\in G^*}\prod_{i=1}^{l}\prod_{b\in B_i} \eta_b(\phi)\right\rfloor \leqslant \left\lfloor \frac{1}{l}\sum_{i=1}^{l}\sum_{\phi\in G^*}\prod_{b\in B_i} \eta_G(b,\phi)^l\right\rfloor \leqslant \mathbf{M}_G(l), \tag{2.46}$$

and that completes the proof. □

Proof of Corollary 1.9. (1) This part follows from Corollary 1.8 and the fact that

$$\mathbf{M}_V(l) = \left\lfloor \left(1+(p-1)\left(\frac{p-2}{p-1}\right)^l\right)^n\right\rfloor. \tag{2.47}$$

To prove equation (2.47), we naturally identify the dual V^* with V and note that if B is a linear basis of V and $v \in V$ then

$$\prod_{b\in B} \eta_V(b,v)^l = \left(\frac{p-2}{p-1}\right)^{l\cdot(\#\text{ of non-zero coordinates of } v \text{ with respect to the basis } B)}. \tag{2.48}$$

Equation (2.47) then follows from the fact that, for $t \in \{0,\ldots,n\}$, the number of points of V with exactly t non-zero coordinates with respect to the basis B is exactly $\binom{n}{t}(p-1)^t$.

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

(2) To prove that the additive span of $\uplus_{i=1}^{l} B_i$ contains an affine subspace of dimension at least

$$n\left(1-(p-1)^2\left(\frac{p-2}{p-1}\right)^{l-1}\right), \tag{2.49}$$

we note that this is evidently true for $l=0$, and if $l \geqslant 1$ then part (1) of this corollary implies that

$$\left|\text{addspan}\left(\uplus_{i=1}^{l-1} B_i\right)\right| \geqslant \left\lfloor\left(1+(p-1)\left(\frac{p-2}{p-1}\right)^{l-1}\right)^{n}\right\rfloor^{-1} p^n. \tag{2.50}$$

Moreover, the way we prove part (1) of this corollary via Corollaries 1.8, 1.7, and part (1.1) of Theorem (1.1) is by proving that we can find cosets of b° for $b \in \uplus_{i=1}^{l-1} B_i$ such that the complement P_{l-1} of the union of these cosets satisfies

$$1 \leqslant \left|P_{l-1}\right| \leqslant \left\lfloor\left(1+(p-1)\left(\frac{p-2}{p-1}\right)^{l-1}\right)^{n}\right\rfloor. \tag{2.51}$$

We can then finish the proof of part (2) of this corollary in similar fashion to the proof of Corollary 1.5. Suppose that $B_l=\{b_1,\dots,b_n\}$. By Theorem 1.2 applied to the sequence $(b_1,\dots,b_n)$ and the set $P=P_{l-1}$, we can find a subsequence $(b'_1,\dots,b'_{n'})$ of $(b_1,\dots,b_n)$ and cosets $C(b'_1),\dots,C(b'_{n'})$ of $(b'_1)^\circ,\dots,(b'_{n'})^\circ$ such that the set

$$P' = P_{l-1} \setminus \left(\cup_{j=1}^{n'} C(b'_j)\right), \tag{2.52}$$

is contained in a coset of $\langle(b_1,\dots,b_n)\backslash(b'_1,\dots,b'_{n'})\rangle^\circ$ and has size

$$1 \leqslant \left|P'\right| \leqslant \left(\frac{p-2}{p-1}\right)^{n'}\left|P_{l-1}\right| \leqslant \left(\frac{p-2}{p-1}\right)^{n'}\left\lfloor\left(1+(p-1)\left(\frac{p-2}{p-1}\right)^{l-1}\right)^{n}\right\rfloor. \tag{2.53}$$

Equation (2.53) then implies that

$$n' \leqslant n(p-1)^2\left(\frac{p-2}{p-1}\right)^{l-1}. \tag{2.54}$$

So we can find cosets of b° for $b \in \uplus_{i=1}^{l} B_i$ such that the complement of the union of these cosets is non-empty and contained in a coset of $\langle(b_1,\dots,b_n)\backslash(b'_1,\dots,b'_{n'})\rangle^\circ$, and part (1.1) of Theorem 1.1 then implies that the additive span of $\uplus_{i=1}^{l} B_i$ contains a coset of the n'-codimensional (and therefore $(n-n')$-dimensional) linear subspace $\langle(b_1,\dots,b_n)\backslash(b'_1,\dots,b'_{n'})\rangle$. Part (2) of this corollary then follows from equation (2.54).

(3) Note that

$$\text{if } l \geqslant \frac{\ln n+\ln(p-1)-\ln\ln 2}{\ln(p-1)-\ln(p-2)} \text{ then } \left(\frac{p-1}{p-2}\right)^{l} \geqslant \frac{n(p-1)}{\ln 2}, \tag{2.55}$$

and since $\ln 2$ is irrational the latter inequality is strict, implying that $\mathbf{M}_V(l)<2$, so (since $\mathbf{M}_V(l)$ is an integer) $\mathbf{M}_V(l)=1$, which together with part (1) of this corollary completes the proof. □

Remark. The proof of part (2) of Corollary 1.9 implies that, for each $i \in \{1,\dots,l\}$, there exists a subset $B'_i \subseteq B_i$ consisting of at least

$$n\left(1-(p-1)^2\left(\frac{p-2}{p-1}\right)^{l-1}\right), \tag{2.56}$$

elements such that the additive span of $\uplus_{i=1}^{l} B_i$ contains a translate of the linear span of B'_i. So we can give a somewhat more concrete description of the affine subspace satisfying part (2) of Corollary 1.9.

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press

References

[1] Alon, N., Linial, N. and Meshulam, R. (1991) Additive bases of vector spaces over prime fields. *J. Comb. Theory Ser. A.* **57** 203–210.
[2] Hatami, H. and de Quehen, V. (2016) On the additive bases problem in finite fields. *Electron. J. Comb.* **23**(3) P3.33.
[3] Jaeger, F., Linial, N., Payan, C. and Tarsi, M. (1992) Group connectivity of graphs—A nonhomogeneous analogue of nowhere-zero flow properties. *J. Comb. Theory Ser. B* **56** 165–182.
[4] Lev, V. F., Muzychuk, M. E. and Pinchasi, R. (2010) Additive bases in abelian groups, *Int. J. Number Theory* **6**(4) 799–809.
[5] Tao, T. (2005) An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.* **12**(1) 121–127.

Cite this article: Arsovski B (2021). Additive bases via Fourier analysis. *Combinatorics, Probability and Computing* **30**, 930–941. https://doi.org/10.1017/S0963548321000109

https://doi.org/10.1017/S0963548321000109 Published online by Cambridge University Press