ADDITIVE BASES IN ABELIAN GROUPS

VSEVOLOD F. LEV, MIKHAIL E. MUZYCHUK, AND ROM PINCHASI

Abstract. Let G be a finite, non-trivial abelian group of exponent m, and suppose that $B_1, \dots, B_k$ are generating subsets of G. We prove that if $k > 2m \ln \log_2 |G|$, then the multiset union $B_1 \cup \dots \cup B_k$ forms an additive basis of G; that is, for every $g \in G$ there exist $A_1 \subseteq B_1, \dots, A_k \subseteq B_k$ such that $g = \sum_{i=1}^{k} \sum_{a \in A_i} a$. This generalizes a result of Alon, Linial, and Meshulam on the additive bases conjecture.

As another step towards proving the conjecture, in the case where $B_1, \dots, B_k$ are finite subsets of a vector space we obtain lower-bound estimates for the number of distinct values, attained by the sums of the form $\sum_{i=1}^{k} \sum_{a \in A_i} a$, where A_i vary over all subsets of B_i for each $i = 1, \dots, k$.

Finally, we establish a surprising relation between the additive bases conjecture and the problem of covering the vertices of a unit cube by translates of a lattice, and present a reformulation of (the strong form of) the conjecture in terms of coverings.

1. Introduction and statement of the results

Given an abelian group G and a multiset $B = \{b_1, \dots, b_n\} \subseteq G$, we say that B is an *additive basis* of G if for every group element $g \in G$ there exists an index set $I \subseteq [1, n]$ such that $g = \sum_{i \in I} b_i$.

Jaeger et al conjectured in [JLPT92] that for any prime p there is an integer $k(p) > 0$ with the property that if $B_1, \dots, B_{k(p)}$ are (linear) bases of the finite-dimensional vector space V over the p-element field, then the multiset union $B_1 \cup \dots \cup B_{k(p)}$ is an additive basis of V. This statement is known as the *additive basis conjecture*. Alon et al proved in [ALM91], in two different ways, that there exists a function $c(p)$ such that if $|V| = p^n$, $k > c(p) \ln n$, and $B_1, \dots, B_k$ are bases of V, then the multiset union $B_1 \cup \dots \cup B_k$ is an additive basis of V. One of their proofs, using the polynomial method and properties of the permanent, shows that $B_1 \cup \dots \cup B_k$ is an additive basis of V, provided that $k \geq (p-1) \ln n + p - 2$; another proof, using exponential sums, requires $k \geq (p^2/2) \ln 2pn + 1$. In this paper we introduce yet another approach allowing us to establish the following generalization.

Theorem 1. *Let G be a finite, non-trivial abelian group of exponent m, and suppose that $B_1, \dots, B_k$ are generating subsets of G. If $k > 2m \ln \log_2 |G|$, then the multiset union $B_1 \cup \dots \cup B_k$ is an additive basis of G.*

Our argument is based on the following interpretation of the problem. For a subset B of an abelian group G write

$$B^* := \left\{ \sum_{a\in A} a \colon A \subseteq B,\ |A| < \infty \right\}$$

(the *subset sum set* of B), and given subsets $B_1, \dots, B_k \subseteq G$ let

$$B_1 + \dots + B_k := \{b_1 + \dots + b_k \colon b_1 \in B_1, \dots, b_k \in B_k\}$$

(the *sumset* of $B_1, \dots, B_k$). Clearly, in order for the multiset union $B_1 \cup \dots \cup B_k$ to form an additive basis of G, it is necessary and sufficient that $B_1^* + \dots + B_k^* = G$. Accordingly, Theorem 1 can be equivalently restated as follows.

Theorem 1′. *Let G be a finite, non-trivial abelian group of exponent m, and suppose that $B_1, \dots, B_k$ are generating subsets of G. If $k > 2m \ln \log_2 |G|$, then $B_1^* + \dots + B_k^* = G$.*

We notice that if $B_1, \dots, B_k$ are bases of a vector space, then the sumset $B_1^* + \dots + B_k^*$ has a transparent geometric meaning: namely, it is the Minkowski sum of the vertex sets of the parallelepipeds, spanned by $B_1, \dots, B_k$. One may hope that studying sumsets of this form can eventually lead to a proof of the additive basis conjecture. We establish two results in this direction.

Theorem 2. *Let k be a positive integer. If $B_1, \dots, B_k$ are finite, non-empty subsets of the vector space V over a field of infinite characteristic, then*

$$|B_1^* + \dots + B_k^*| \ge 2^{\mathrm{rk}(B_1)}\, (3/2)^{\mathrm{rk}(B_2)} \cdots ((k+1)/k)^{\mathrm{rk}(B_k)}.$$

In particular, if $\dim V = n$ and $B_1, \dots, B_k$ are bases of V, then

$$|B_1^* + \dots + B_k^*| \ge (k+1)^n.$$

Notice, that in the second estimate of the theorem equality is attained if $B_1 = \dots = B_k$.

Theorem 3. *If B_1 and B_2 are finite subsets of a vector space V over a field of infinite or odd characteristic, then*

$$|B_1^* + B_2^*| \ge \left(\frac{8}{3}\right)^{(\mathrm{rk}(B_1)+\mathrm{rk}(B_2))/2}.$$

In particular, if $\dim V = n$ and B_1, B_2 are bases of V, then

$$|B_1^* + B_2^*| \ge \left(\frac{8}{3}\right)^n.$$

It is difficult to expect that the constant $8/3$ is best possible in this context. On the other hand, it cannot be replaced by a value larger than $\sqrt{8}$, at least for the underlying field of characteristic 3: for, if V is an even-dimension vector space over such a field, and if $B_1 = \{e_1, \dots, e_{2l}\}$ is a basis of V, then for the basis

$$B_2 := \{e_1 + e_2, e_1 - e_2,\ e_3 + e_4, e_3 - e_4, \dots, e_{2l-1} + e_{2l}, e_{2l-1} - e_{2l}\}$$

we have $|B_1^* + B_2^*| = 8^l$.

Yet another, completely different approach is presented in Section 3, where the additive bases conjecture is interpreted in terms of coverings of the vertices of the unit cube by translates of an integer lattice. We postpone the discussion and exact statement of the result to avoid aggregating notation and terminology at this stage.

2. The proofs

Proof of Theorem 1′. For $m = 2$ the assertion is immediate, as in this case $B^* = G$ for any generating subset $B \subseteq G$. Assume for the rest of the proof that $m \geq 3$, and for $j \in [1, k]$ let $S_j := B_1^* + \dots + B_j^*$.

The key ingredient of our argument is the Ruzsa sum triangle inequality, which says that for any positive integer n and any finite subsets $A_0, A_1, \dots, A_n$ of an abelian group one has

$$|A_0|^{n-1}|A_1 + \dots + A_n| \leq |A_0 + A_1| \cdots |A_0 + A_n|;$$

see, for instance, [**?**, Theorem 12.34]. Applying this inequality with $n = m - 1$, $A_0 = S_{j-1}$, and $A_1 = \dots = A_n = B_j^*$, we obtain

$$|S_{j-1}|^{m-2}|(m-1)B_j^*| \leq |S_{j-1} + B_j^*|^{m-1}; \quad j \in [2, k].$$

As $(m-1)B_j^* = G$ and $S_{j-1} + B_j^* = S_j$, we derive that

$$|S_j| \geq |S_{j-1}|^{1-\frac{1}{m-1}}|G|^{\frac{1}{m-1}}$$

and consequently

$$\frac{|G|}{|S_j|} \leq \left(\frac{|G|}{|S_{j-1}|}\right)^{1-\frac{1}{m-1}}$$

for every $j \in [2, k]$. Iterating, we obtain

$$\ln \frac{|G|}{|S_j|} \leq \left(1 - \frac{1}{m-1}\right)^{j-1} \ln \frac{|G|}{|S_1|} \leq e^{-\frac{j-1}{m}} \ln \frac{|G|}{|S_1|}; \quad j \in [1, k].$$

Let r denote the rank of G. Since $|G| \leq m^r$ and $|S_1| = |B_1^*| \geq 2^r$ (for if C is a minimal generating subset of B_1, then $|B_1^*| \geq |C^*| = 2^{|C|} \geq 2^r$), using some basic

calculus it is not difficult to deduce that

$$\ln \frac{|G|}{|S_j|} < e^{-\frac{j+1}{m}} \ln |G|; \quad j \in [1,k].$$

Thus, if $j = \lfloor m \ln \log_2 |G| \rfloor$ (so that $k > 2j > 0$), then

$$|B_1^* + \cdots + B_j^*| = |S_j| > \frac{1}{2}\,|G|,$$

and similarly

$$|B_{j+1}^* + \cdots + B_{2j}^*| > \frac{1}{2}\,|G|.$$

We now use the fact that if two sets $S, T \subseteq G$ satisfy $|S| + |T| > |G|$, then for any element $g \in G$ the sets S and $g - T$ have non-empty intersection in view of

$$|S \cap (g-T)| = |S| + |g-T| - |S \cup (g-T)| \ge |S| + |T| - |G| > 0;$$

hence $g \in S+T$ and therefore $S+T = G$. Applying this to the sets $S := B_1^* + \cdots + B_j^*$ and $T := B_{j+1}^* + \cdots + B_{2j}^*$, we get

$$B_1^* + \cdots + B_{2j}^* = G,$$

which implies the result. □

Proof of Theorem 2. We use induction on k, and for any fixed value of k induction on

$$\min\{\mathrm{rk}(B_1), \ldots, \mathrm{rk}(B_k)\}.$$

The case $k = 1$ follows from the observation that if $r = \mathrm{rk}(B_1)$ and $b_1, \ldots, b_r \in B_1$ are linearly independent, then all 2^r sums

$$\textstyle\sum_{i \in I} b_i; \quad I \subseteq [1,r]$$

are pairwise distinct. The case where $k \ge 2$ and $\min\{\mathrm{rk}(B_1), \ldots, \mathrm{rk}(B_k)\} = 0$ follows easily by the induction hypothesis. Suppose, therefore, that $k \ge 2$ and $\mathrm{rk}(B_1), \ldots, \mathrm{rk}(B_k)$ are all positive. Fix arbitrarily $b \in B_k$ and write $B_0 := B_k \setminus \{b\}$. Choose a linear subspace L complementing $\mathrm{Sp}\,\{b\}$ to the whole vector space, and let π denote the projection onto L along b. We have then

$$B_1^* + \cdots + B_k^* = (B_1^* + \cdots + B_{k-1}^* + B_0^*) \cup (B_1^* + \cdots + B_{k-1}^* + B_0^* + b),$$

and since

$$\begin{aligned} |(B_1^* + \cdots + B_{k-1}^* + B_0^* + b) \setminus (B_1^* + \cdots + B_{k-1}^* + B_0^*)| \\ \ge |\pi(B_1^* + \cdots + B_{k-1}^* + B_0^*)| = |(\pi(B_1))^* + \cdots + (\pi(B_k))^*|, \end{aligned}$$

it follows by the induction hypothesis (and in view of $\mathrm{rk}(B_0) \geq \mathrm{rk}(B_k) - 1$ and $\mathrm{rk}(\pi(B)) \geq \mathrm{rk}(B) - 1$, for any vector set B) that

$$\begin{aligned}|B_1^* + \cdots + B_k^*| &= |B_1^* + \cdots + B_{k-1}^* + B_0^*| \\ &\qquad + |(B_1^* + \cdots + B_{k-1}^* + B_0^* + b) \setminus (B_1^* + \cdots + B_{k-1}^* + B_0^*)| \\ &\geq \prod_{j=1}^{k-1} \left(1 + \frac{1}{j}\right)^{\mathrm{rk}(B_j)} \cdot \left(1 + \frac{1}{k}\right)^{\mathrm{rk}(B_k)-1} + \prod_{j=1}^{k} \left(1 + \frac{1}{j}\right)^{\mathrm{rk}(B_j)-1} \\ &= \prod_{j=1}^{k} \left(1 + \frac{1}{j}\right)^{\mathrm{rk}(B_j)},\end{aligned}$$

as desired. □

For a finite subset B of an abelian group, let

$$T(B) := \{(b_1, b_2, b_3, b_4) \in B \times B \times B \times B \colon b_1 + b_2 = b_3 + b_4\}.$$

The proof of Theorem 3 is based on

Proposition 1. *For any finite, non-empty subsets A and B of an abelian group we have*

$$|A + B| \geq \frac{|A|^2 |B|^2}{\sqrt{T(A)T(B)}}.$$

Proof. For a group element z write

$$\begin{aligned}\nu_{A-A}(z) &:= |\{(a_1, a_2) \in A \times A \colon z = a_1 - a_2\}|, \\ \nu_{B-B}(z) &:= |\{(b_1, b_2) \in B \times B \colon z = b_1 - b_2\}|,\end{aligned}$$

and

$$\nu_{A+B}(z) := |\{(a, b) \in A \times B \colon z = a + b\}|.$$

By the Cauchy-Schwarz inequality, we have

$$\frac{|A|^2 |B|^2}{|A + B|} = \frac{1}{|A + B|} \left(\sum_z \nu_{A+B}(z)\right)^2 \leq \sum_z \big(\nu_{A+B}(z)\big)^2.$$

The sum in the right-hand side is the number of solutions of the equation $x_1 + y_1 = x_2 + y_2$ in the variables $x_1, x_2 \in A$ and $y_1, y_2 \in B$. Rewriting this equation as

$x_1 - x_2 = y_2 - y_1$ we see that the number of its solutions is equal to

$$\sum_z \nu_{A-A}(z)\nu_{B-B}(z) \le \left(\sum_z \big(\nu_{A-A}(z)\big)^2\right)^{1/2} \left(\sum_z \big(\nu_{B-B}(z)\big)^2\right)^{1/2} = \sqrt{T(A)T(B)},$$

and the result follows. □

Proof of Theorem 3. Removing dependent vectors from the sets B_i, we assume without loss of generality that $\mathrm{rk}(B_i) = |B_i|$ and $|B_i^*| = 2^{|B_i|}$ for $i \in \{1, 2\}$. We apply Proposition 1 to the sets B_1^* and B_2^*. The quantities $T(B_i^*)$ can be explicitly calculated as follows. For a group element z let

$$\nu_i(z) := |\{(b', b'') \in B_i^* \times B_i^* \colon z = b' - b''\}|; \quad i \in \{1, 2\},$$

so that

$$T(B_i^*) = \sum_{z \in B_i^* - B_i^*} (\nu_i(z))^2.$$

Fix $i \in \{1, 2\}$, set $n := |B_i|$, and write $B_i = \{b_1, \dots, b_n\}$. The condition $z \in B_i^* - B_i^*$ means that $z = \varepsilon_1 b_1 + \dots + \varepsilon_n b_n$ with $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 0, 1\}$, and it is easily seen that in this case

$$\nu_i(z) = 2^{n - |\varepsilon_1| - \dots - |\varepsilon_n|}.$$

Consequently, we have

$$\begin{aligned} T(B_i^*) &= \sum_{\varepsilon_1, \dots, \varepsilon_n = -1}^{1} 2^{2n - 2|\varepsilon_1| - \dots - 2|\varepsilon_n|} \\ &= 2^{2n} \prod_{i=1}^{n} \sum_{\varepsilon_i = -1}^{1} 2^{-2|\varepsilon_i|} \\ &= 6^n \end{aligned}$$

and it follows that

$$|B_1^* + B_2^*| \ge \frac{2^{2|B_1| + 2|B_2|}}{\sqrt{6^{|B_1| + |B_2|}}} = \left(\frac{8}{3}\right)^{(|B_1| + |B_2|)/2} = \left(\frac{8}{3}\right)^{(\mathrm{rk}(B_1) + \mathrm{rk}(B_2))/2}.$$

□

We remark that the approach used in the proof of Proposition 1 can be combined with character sum technique in the spirit of [ALM91], to show that for any system of

bases $B_1, \dots, B_k$ of an r-dimensional vector space over a field of finite characteristic $p > 2$ one has

$$|B_1^* + \cdots + B_k^*| \ge \frac{p^r}{(1+\sigma_p(k))^r},$$

where

$$\sigma_p(k) = \sum_{u=1}^{p-1} \left(\cos \pi \frac{u}{p}\right)^{2k}.$$

(Hint for the interested reader: if $\nu(g)$ denotes the number of representations of the vector g in the form $g = b_1 + \cdots + b_k$ with $b_i \in B_i^*$ for $i \in [1,k]$, then the sum $\sum_g (\nu(g))^2$ counts the number of $2k$-tuples $(x_1, \dots, x_k, y_1, \dots, y_k)$ with $x_1 + \cdots + x_k = y_1 + \cdots + y_k$ and $x_i, y_i \in B_i^*$ for $i \in [1,k]$. This number is easily expressed using character sums.) Since $1 + \sigma_p(2) = 3p/8$ for any prime $p > 2$, the estimate above extends the result of Theorem 3.

3. Additive bases via lattice coverings

Suppose that $k \ge 2$ and $r \ge 1$ are fixed integers. Given a prime p, we say that a lattice in $\mathbb{Z}^{kr}$ is *p-oblique* if, whenever for some $i_0 \in [1,k]$ a lattice vector

$$(z_{11}, \dots, z_{1r}, \dots, z_{k1}, \dots, z_{kr})$$

satisfies

$$z_{ij} \equiv 0 \pmod p \quad \text{for all } i \in [1,k] \setminus \{i_0\},\ j \in [1,r],$$

it also satisfies

$$z_{i_0 j} \equiv 0 \pmod p \quad \text{for all } j \in [1,r].$$

(The term *oblique* is meant as an indication that the lattice is not aligned with the coordinate hyperplanes.) Furthermore, we define the *covering number* of a lattice $\Lambda \le \mathbb{Z}^{kr}$ to be the minimal number of translates of Λ, containing in their union all vertices of the unit cube $[0,1]^{kr}$, and we denote this quantity by $C(\Lambda)$; thus,

$$C(\Lambda) = \min\{|S| \colon S \subseteq \mathbb{Z}^{kr},\ \{0,1\}^{kr} \subseteq S + \Lambda\}.$$

We conclude this paper with the following, somewhat surprising, result.

Theorem 4. *For any integer $k \ge 2$ and $r \ge 1$, prime p, and field $\mathbb{F}$ of characteristic p, we have*

$$\min_{B_1,\dots,B_k \subseteq \mathbb{F}^r} |B_1^* + \cdots + B_k^*| \ge \min_{\Lambda \le \mathbb{Z}^{kr}} C(\Lambda),$$

where the minimum in the left-hand side extends over all systems of k bases of $\mathbb{F}^r$, and in the right-hand side over all p-oblique lattices in $\mathbb{Z}^{kr}$. If $k \le |\mathbb{F}|$ then, indeed,

equality holds; moreover, in this case there is a p-oblique lattice $p\mathbb{Z}^{kr} \le \Lambda \le \mathbb{Z}^{kr}$ with $\det\Lambda = p^r$, on which the minimum in the right-hand side is attained.

Remark. It is not clear to us to what extent the condition $k \le |\mathbb{F}|$ is essential and whether the assertion of Theorem 4 fails in a critical way if this condition is dropped.

We notice that if k, r, and p are as in Theorem 4, then the lattice Λ of all integer vectors $(z_{11}, \dots, z_{kr})$ with

$$z_{1j} + \dots + z_{kj} \equiv 0 \pmod{p}; \quad j = 1, \dots, r$$

has covering number $C(\Lambda) = \min\{(k+1)^r, p^r\}$. To see this, observe that different translates of Λ correspond in a natural way to integer vectors of the form $(z_{11}, \dots, z_{1r}, 0, \dots, 0)$ with $z_{11}, \dots, z_{1r} \in [0, p-1]$, and on the other hand, such a vector is congruent modulo Λ to a vector from $\{0,1\}^{kr}$ if and only if $z_{11}, \dots, z_{1r} \le k$.

By Theorem 4, the additive bases conjecture will follow if one can show that there are no p-oblique lattices with the covering number smaller than p^r; that is, to show that for any prime p there exists an integer $k = k(p) > 0$ such that the set $\{0,1\}^{kr}$ cannot be covered by fewer than p^r translates of a p-oblique lattice, for any integer $r \ge 1$. By all we know, the conjecture may even be true with $k(p) = p$. Theorem 4 shows this strong form of the conjecture is equivalent to the assertion that one cannot cover the set $\{0,1\}^{pr}$ by fewer than p^r translates of a p-oblique lattice.

Proof of Theorem 4. Suppose that $\mathcal{B} = \{B_1, \dots, B_k\}$ is a system of bases of $\mathbb{F}^r$. We write

$$B_i = \{b_{i1}, \dots, b_{ir}\}; \quad i = 1, \dots, k$$

and define a linear mapping $\varphi_{\mathcal{B}} \colon \mathbb{Z}^{kr} \to \mathbb{F}^r$ by

$$\varphi_{\mathcal{B}}(x_{11}, \dots, x_{kr}) = x_{11}b_{11} + \dots + x_{1r}b_{1r} + \dots + x_{k1}b_{k1} + \dots + x_{kr}b_{kr},$$

so that the sumset $B_1^* + \dots + B_k^*$ is the image of $\{0,1\}^{kr}$ under $\varphi_{\mathcal{B}}$.

Let $\Lambda_{\mathcal{B}} := \ker\varphi_{\mathcal{B}}$; thus, $\Lambda_{\mathcal{B}}$ is a sublattice of $\mathbb{Z}^{kr}$, lying above $p\mathbb{Z}^{kr}$, and hence a full-rank sublattice. From the fact that for any integer $x_{11}, \dots, x_{k-1,r}$ there are unique $x_{k1}, \dots, x_{kr} \in [0, p)$ with $(x_{11}, \dots, x_{kr}) \in \Lambda_{\mathcal{B}}$, it follows that $\det\Lambda_{\mathcal{B}} = p^r$. Furthermore, $\Lambda_{\mathcal{B}}$ is (evidently) p-oblique.

Since for $u, v \in \mathbb{Z}^{kr}$, and in particular for $u, v \in \{0,1\}^{kr}$, the equality $\varphi_{\mathcal{B}}(u) = \varphi_{\mathcal{B}}(v)$ is equivalent to $v \equiv u \pmod{\Lambda_{\mathcal{B}}}$, we have

$$|B_1^* + \dots + B_k^*| = |\varphi_{\mathcal{B}}(\{0,1\}^{kr})| = C(\Lambda_{\mathcal{B}}).$$

This proves the first assertion of the theorem, and to complete the proof we assume that $k \le |\mathbb{F}|$ and show that for every p-oblique lattice $\Lambda \le \mathbb{Z}^{kr}$ there exists a system $\mathcal{B}$ of k bases of $\mathbb{F}^r$ with $\Lambda_{\mathcal{B}} \ge \Lambda$ and consequently, with $C(\Lambda_{\mathcal{B}}) \le C(\Lambda)$.

Replacing Λ with $\Lambda + p\mathbb{Z}^{kr}$ we can assume that Λ is of full rank. Let $\mathbb{Z}^{kr} = V_1 \oplus \cdots \oplus V_k$, where V_i is the rank-r sublattice, spanned over $\mathbb{Z}$ by the "ith coordinate block" (for each $i = 1, \dots, k$), fix a basis $\{l^{(1)}, \dots, l^{(kr)}\}$ of Λ, and for each $t \in [1, kr]$ consider the decomposition

$$l^{(t)} = l_1^{(t)} + \cdots + l_k^{(t)}; \quad l_i^{(t)} \in V_i \ \text{ for } i = 1, \dots, k.$$

What we want $\mathcal{B}$ to satisfy is that $\varphi_{\mathcal{B}}(l^{(t)}) = 0$ for every $t \in [1, kr]$. Writing $\mathcal{B} = \{B_1, \dots, B_k\}$ and $B_i = \{b_{i1}, \dots, b_{ir}\}$ for each $i = 1, \dots, k$, the condition to secure takes the shape

$$\mathsf{B}_1 l_1^{(t)} + \cdots + \mathsf{B}_k l_k^{(t)} = 0; \quad t \in [1, kr],$$

where B_i is the $r \times r$ matrix over $\mathbb{F}$, whose columns are formed by the vectors $b_{i1}, \dots, b_{ir}$. Thus, if for each $i = 1, \dots, k$ by L_i we denote the $r \times kr$ matrix over $\mathbb{Z}$, whose columns are formed by the vectors $l_i^{(1)}, \dots, l_i^{(kr)}$, then what we ultimately want to prove is the existence of $\mathsf{B}_1, \dots, \mathsf{B}_k \in \mathrm{GL}_r(\mathbb{F})$ satisfying $\mathsf{B}_1\mathsf{L}_1 + \cdots + \mathsf{B}_k\mathsf{L}_k = 0$.

We notice that the matrices L_i actually have integer entries, but we treat them in the last equality, and will continue to treat for the rest of the proof, as matrices over the p-element field $\mathbb{F}_p \le \mathbb{F}$, and we also seek B_i with the entries in $\mathbb{F}_p$. With this convention, the assumption that Λ is p-oblique (which has not been used yet) guarantees that for each $i \in [1, k]$, the intersection

$$\ker \mathsf{L}_1 \cap \cdots \cap \ker \mathsf{L}_{i-1} \cap \ker \mathsf{L}_{i+1} \cap \cdots \cap \ker \mathsf{L}_k$$

is contained in $\ker \mathsf{L}_i$. The proof is concluded by using

Proposition 2. *Suppose that $r, n \ge 1$ and $k \ge 2$ are integers and $\mathsf{L}_1, \dots, \mathsf{L}_k$ are matrices of size $r \times n$ over a field $\mathbb{F}$ with $|\mathbb{F}| \ge k$. If for each $i \in [1, k]$ we have*

$$\bigcap_{j \in [1,k]\colon j \ne i} \ker \mathsf{L}_j \subseteq \ker \mathsf{L}_i,$$

then there exist matrices $\mathsf{B}_1, \dots, \mathsf{B}_k \in \mathrm{GL}_r(\mathbb{F})$ satisfying

$$\mathsf{B}_1\mathsf{L}_1 + \cdots + \mathsf{B}_k\mathsf{L}_k = 0.$$

The proof of Proposition 2 is presented in the Appendix. □

Appendix: Proof of Proposition 2.

The assumptions $\bigcap_{j\in[1,k]:\, j\neq i} \ker \mathsf{L}_j \subseteq \ker \mathsf{L}_i$ shows that if a vector in $\mathbb{F}^n$ is orthogonal to every row of every matrix L_j with $j \in [1,k]\setminus\{i\}$, then it is also orthogonal to every row of the matrix L_i; in other words, every row of L_i is a linear combination of the rows of L_j for $j \in [1,k]\setminus\{i\}$. Thus, there exist matrices A_{ij} of size $r\times r$ over the field $\mathbb{F}$, for each pair of indices $i,j\in[1,k]$ with $i\neq j$, such that

$$\mathsf{L}_i = \sum_{j\in[1,k]:\, j\neq i} \mathsf{A}_{ij}\mathsf{L}_j; \quad i\in[1,k].$$

For $i\in[1,k]$ we define $A_{ii} := -\mathsf{I}_r$, where I_r is the identity matrix of size $r\times r$, to get

$$\mathsf{A}_{i1}\mathsf{L}_1 + \cdots + \mathsf{A}_{ik}\mathsf{L}_k = 0; \quad i\in[1,k].$$

(The reader may find it useful to consider the matrices A_{ij} being organized themselves into a $k\times k$ matrix, and the matrices $\mathsf{L}_1,\dots,\mathsf{L}_k$ written as a "column vector".)

If we can find matrices $\mathsf{M}_1,\dots,\mathsf{M}_k$ of size $r\times r$ so that none of the linear combinations

$$\mathsf{B}_j := \mathsf{M}_1\mathsf{A}_{1j} + \cdots + \mathsf{M}_k\mathsf{A}_{kj}; \quad j\in[1,k]$$

is degenerate, then we are done in view of

$$\sum_{j=1}^{k} \mathsf{B}_j\mathsf{L}_j = \sum_{i=1}^{k} \mathsf{M}_i \sum_{j=1}^{k} \mathsf{A}_{ij}\mathsf{L}_j = 0.$$

We complete the proof of the proposition establishing the existence of such matrices $\mathsf{M}_1,\dots,\mathsf{M}_k$.

Lemma 1. *Suppose that $r,k\geq 1$ are integers and that A_{ij} $(i,j\in[1,k])$ are matrices of size $r\times r$ over a field $\mathbb{F}$ such that A_{ii} is non-degenerate for each $i\in[1,k]$. If $|\mathbb{F}|\geq k$, then there exist matrices $\mathsf{M}_1,\dots,\mathsf{M}_k$ over $\mathbb{F}$ of size $r\times r$ so that none of*

$$\mathsf{M}_1\mathsf{A}_{1j} + \cdots + \mathsf{M}_k\mathsf{A}_{kj}; \quad j\in[1,k]$$

is degenerate.

Proof. We use induction on k. The case $k=1$ trivial; suppose that $k\geq 2$.

If $\mathsf{A}_{k1},\dots,\mathsf{A}_{k\,k-1}$ are all non-degenerate, then we can take $\mathsf{M}_1 = \cdots = \mathsf{M}_{k-1} = 0$ and $\mathsf{M}_k = \mathsf{I}_r$. Assume therefore that one of the matrices A_{ki} with $i\in[1,k-1]$, say A_{k1}, *is* degenerate. Applying the induction hypothesis, find $\mathsf{M}_1,\dots,\mathsf{M}_{k-1}$ so that

$$\mathsf{B}_j := \mathsf{M}_1\mathsf{A}_{1j} + \cdots + \mathsf{M}_{k-1}\mathsf{A}_{k-1\,j}; \quad j\in[1,k-1]$$

are non-degenerate, and let

$$\mathsf{B}_k := \mathsf{M}_1\mathsf{A}_{1k} + \cdots + \mathsf{M}_{k-1}\mathsf{A}_{k-1\,k}.$$

Recalling that A_{1k}, and thus also $\mathsf{A}_{1k}\mathsf{B}_1^{-1}$, are degenerate, we find $\mathsf{U}, \mathsf{V} \in \mathrm{GL}_r(\mathbb{F})$ so that the matrix $\mathsf{V}\mathsf{A}_{1k}\mathsf{B}_1^{-1}\mathsf{U}$ is upper-triangular with zeroes on the main diagonal, and we seek M_k in the form $\mathsf{M}_k = \mathsf{U}\mathsf{D}\mathsf{V}$ with a diagonal matrix D. Thus, D is to be found so that none of $\mathsf{B}_j + \mathsf{U}\mathsf{D}\mathsf{V}\mathsf{A}_{kj}$ for $j \in [1, k]$ are degenerate. Since

$$\mathsf{B}_1 + \mathsf{U}\mathsf{D}\mathsf{V}\mathsf{A}_{k1} = \mathsf{U}(\mathsf{I}_r + \mathsf{D}\cdot\mathsf{V}\mathsf{A}_{1k}\mathsf{B}_1^{-1}\mathsf{U})\mathsf{U}^{-1}\mathsf{B}_1,$$

this matrix is non-degenerate. Therefore, it remains to show that there is a diagonal matrix D such that

$$\mathsf{B}_2 + \mathsf{U}\mathsf{D}\mathsf{V}\mathsf{A}_{k2}, \ldots, \mathsf{B}_k + \mathsf{U}\mathsf{D}\mathsf{V}\mathsf{A}_{kk}$$

are non-degenerate.

To this end we consider the polynomial in r variables over the field $\mathbb{F}$, defined by

$$P(t_1, \ldots, t_r) := \prod_{j=2}^{k} \det(\mathsf{B}_j + \mathsf{U}\mathsf{D}\mathsf{V}\mathsf{A}_{kj}); \quad \mathsf{D} = \mathrm{diag}(t_1, \ldots, t_r).$$

This is a non-zero polynomial, as each factor is distinct from 0: indeed, the coefficient of $t_1 \cdots t_r$ in the last factor is $\det(\mathsf{U}\mathsf{V}\mathsf{A}_{kk}) \neq 0$, and for each $j \in [2, k-1]$ the constant term of the jth factor is $\det(\mathsf{B}_j) \neq 0$. Furthermore, each factor is linear in every variable t_i; hence the degree of P in every variable is $k-1$. It is well-known, however, that a non-zero polynomial in r variables cannot vanish on a cartesian product of r sets, provided that the cardinality of each set exceeds the degree of the polynomial in the corresponding variable; see, for instance, [AT92, Lemma 2.1]. This implies the existence of $t_1, \ldots, t_r \in \mathbb{F}$ with $P(t_1, \ldots, t_r) \neq 0$, and hence the existence of D with the required property. □

References

[ALM91] N. Alon, N. Linial, and R. Meshulam, Additive Bases of Vector Spaces over Prime Fields, *J. Comb. Theory, Ser. A* **57** (1991), 203–210.

[AT92] N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica* **12** (1992), 125–134.

[JLPT92] F. Jaeger, N. Linial, C. Payan, and M. Tarzi, Group connectivity of graphs — a non-homogenious analogue of nowhere-zero flow, *J. Comb. Theory, Ser. B* **56** (2) (1992), 165–182.

[R89] I.Z. Ruzsa, An application of graph theory to additive number theory, *Sci. Ser. A Math. Sci. (N.S.)* **3** (1989), 97–109.

E-mail address: seva@math.haifa.ac.il

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel

E-mail address: muzy@netanya.ac.il

Department of Computer Science and Mathematics, Netanya Academic College, Netanya 42365, Israel

E-mail address: room@math.technion.ac.il

Department of Mathematics, Technion — Israel Institute of Technology, Haifa 32000, Israel