ADDITIVE BASES AND FLOWS IN GRAPHS

LOUIS ESPERET, RÉMI DE JOANNIS DE VERCLOS, TIEN-NAM LE, AND STÉPHAN THOMASSÉ

Abstract. It was conjectured by Jaeger, Linial, Payan, and Tarsi in 1992 that for any prime number $p$, there is a constant $c$ such that for any $n$, the union (with repetition) of the vectors of any family of $c$ linear bases of $\mathbb{Z}_p^n$ forms an additive basis of $\mathbb{Z}_p^n$ (i.e. any element of $\mathbb{Z}_p^n$ can be expressed as the sum of a subset of these vectors). In this note, we prove this conjecture when each vector contains at most two non-zero entries. As an application, we prove several results on flows in highly edge-connected graphs, extending known results. For instance, assume that $p \geq 3$ is a prime number and $\vec{G}$ is a directed, highly edge-connected graph in which each arc is given a list of two distinct values in $\mathbb{Z}_p$. Then $\vec{G}$ has a $\mathbb{Z}_p$-flow in which each arc is assigned a value of its own list.

1. Introduction

Graphs considered in this paper may have multiple edges but no loops. An additive basis $B$ of a vector space $F$ is a multiset of elements from $F$ such that for all $\beta \in F$, there is a subset of $B$ which sums to $\beta$. Let $\mathbb{Z}_p^n$ be the $n$-dimensional linear space over the prime field $\mathbb{Z}_p$. The following result is a simple consequence of the Cauchy-Davenport Theorem [5] (see also [2]).

Theorem 1 ([5]). For any prime $p$, any multiset of $p - 1$ non-zero elements of $\mathbb{Z}_p$ forms an additive basis of $\mathbb{Z}_p$.

This result can be rephrased as: for $n = 1$, any family of $p - 1$ linear bases of $\mathbb{Z}_p^n$ forms an additive basis of $\mathbb{Z}_p^n$. A natural question is whether this can be extended to all integers $n$. Given a collection of sets $X_1, ..., X_k$, we denote by $\bigcup_{i=1}^k X_i$ the union with repetitions of $X_1, ..., X_k$. Jaeger, Linial, Payan and Tarsi [12] conjectured the

---

The authors are partially supported by ANR Project STINT (ANR-13-BS02-0007) and GATO (ANR-16-CE40-0009-01), and LabEx PERSYVAL-Lab (ANR-11-LABX-0025). An extended abstract of this work appeared in the proceedings of Eurocomb 2017.
following, a generalization of important results regarding nowhere-zero
flows in graphs.

**Conjecture 2** ([12]). For every prime number $p$, there is a constant $c(p)$ such that for any $t \geq c(p)$ linear bases $B_1, \ldots, B_t$ of $\mathbb{Z}_p^n$, the union $\bigcup_{s=1}^t B_s$ forms an additive basis of $\mathbb{Z}_p^n$.

Alon, Linial and Meshulam [1] proved a weaker version of Conjecture 2, that the union of any $p \lceil \log n \rceil$ linear bases of $\mathbb{Z}_p^n$ contains an additive basis of $\mathbb{Z}_p^n$ (note that their bound depends on $n$). The support of a vector $x = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ is the set of indices $i$ such that $x_i \neq 0$. The shadow of a vector $x$ is the (unordered) multiset of non-zero entries of $x$. Note that sizes of the support and of the shadow of a vector are equal. In this note, we prove that Conjecture 2 holds if the support of each vector has size at most two.

**Theorem 3.** Let $p \geq 3$ be a prime number. For some integer $\ell \geq 1$, consider $t \geq 8\ell(3p - 4) + p - 2$ linear bases $B_1, \ldots, B_t$ of $\mathbb{Z}_p^n$ such that the support of each vector has size at most 2, and at most $\ell$ different shadows of size 2 appear among the vectors of $\mathcal{B} = \bigcup_{s=1}^t B_s$. Then $\mathcal{B}$ forms an additive basis of $\mathbb{Z}_p^n$.

Theorem 3 will be proved in Section 3 using a result of Lovász, Thomassen, Wu and Zhang [15] (Theorem 6 below) on flows in highly edge-connected graphs. It was mentioned to us by one of the referees that Lai and Li [14] established the equivalence between Theorem 6 and Theorem 3 in the special case where all the shadows are equal to $\{-1, +1\} \pmod{p}$.

The number of possibilities for an (unordered) multiset of $\mathbb{Z}_p \setminus \{0\}$ of size 2 is $\binom{p-1}{2} + p - 1 = \binom{p}{2}$. As a consequence, Theorem 3 has the following immediate corollary.

**Corollary 4.** Let $p \geq 3$ be a prime number. For any $t \geq 4\frac{\binom{p}{2}}{2}(3p - 4) + p - 2$ linear bases $B_1, \ldots, B_t$ of $\mathbb{Z}_p^n$ such that the support of each vector has size at most 2, $\bigcup_{s=1}^t B_s$ forms an additive basis of $\mathbb{Z}_p^n$.

Another interesting consequence of Theorem 3 concerns the linear subspace $(\mathbb{Z}_p^n)_0$ of vectors of $\mathbb{Z}_p^n$ whose entries sum to 0 (mod $p$).

**Corollary 5.** Let $p \geq 3$ be a prime number. For any $t \geq 4(p-1)(3p - 4) + p - 2$ linear bases $B_1, \ldots, B_t$ of $(\mathbb{Z}_p^n)_0$ such that the support of each vector has size at most 2, $\bigcup_{s=1}^t B_s$ forms an additive basis of $(\mathbb{Z}_p^n)_0$. 
Proof. Note that for any $1 \leq s \leq t$, the linear basis $B_s$ consists of $n - 1$ vectors, each of which has a support of size 2, and the two elements of the shadow sum to 0 (mod $p$). In particular, at most $\frac{p-1}{2}$ different shadows appear among the vectors of the linear bases $B_1, ..., B_t$. It is convenient to view each $B_s$ as a matrix in which the elements of the basis are column vectors. For each $1 \leq s \leq t$, let $B'_s$ be obtained from $B_s$ by deleting the last row. It is easy to see that $B'_s$ is a linear basis of $\mathbb{Z}_p^{n-1}$. Moreover, at most $\frac{p-1}{2}$ different shadows of size 2 appear among the vectors of the linear bases $B'_1, ..., B'_t$ (note that the removal of the last row may have created vectors with shadows of size 1). In particular, it follows from Theorem 3 that for any vector $\beta = (\beta_1, \ldots, \beta_n) \in (\mathbb{Z}_p^n)_0$, the vector $(\beta_1, \ldots, \beta_{n-1}) \in \mathbb{Z}_p^{n-1}$ can be written as a sum of a subset of elements of $\bigcup_{s=1}^t B'_s$. Clearly, the corresponding subset of elements of $\bigcup_{s=1}^t B_s$ sums to $\beta$. This concludes the proof of Corollary 5. 

In the next section, we explore some consequences of Corollary 5.

2. Orientations and flows in graphs

Let $G = (V, E)$ be a non-oriented graph. An orientation $\vec{G} = (V, \vec{E})$ of $G$ is obtained by giving each edge of $E$ a direction. For each edge $e \in E$, we denote the corresponding arc of $\vec{E}$ by $\vec{e}$, and vice versa. For a vertex $v \in V$, we denote by $\delta^+_G(v)$ the set of arcs of $\vec{E}$ leaving $v$, and by $\delta^-_G(v)$ the set of arcs of $\vec{E}$ entering $v$.

For an integer $k \geq 2$, a mapping $\beta : V \to \mathbb{Z}_k$ is said to be a $\mathbb{Z}_k$-boundary of $G$ if $\sum_{v \in V} \beta(v) \equiv 0$ (mod $k$). Given a $\mathbb{Z}_k$-boundary $\beta$ of $G$, an orientation $\vec{G}$ of $G$ is a $\beta$-orientation if $d^+_G(v) - d^-_G(v) \equiv \beta(v)$ (mod $k$) for every $v \in V$, where $d^+_G(v)$ and $d^-_G(v)$ stand for the out-degree and the in-degree of $v$ in $\vec{G}$.

The following major result was obtained by Lovász, Thomassen, Wu and Zhang [15]:

**Theorem 6.** [15] For any $k \geq 1$, any $6k$-edge-connected graph $G$, and any $\mathbb{Z}_{2k+1}$-boundary $\beta$ of $G$, the graph $G$ has a $\beta$-orientation.

A natural question is whether a weighted counterpart of Theorem 6 exists. Given a graph $G = (V, E)$, a $\mathbb{Z}_k$-boundary $\beta$ of $G$ and a mapping $f : E \to \mathbb{Z}_k$, an orientation $\vec{G}$ of $G$ is called an $f$-weighted $\beta$-orientation if $\partial f(v) \equiv \beta(v)$ (mod $k$) for every $v$, where $\partial f(v) = \sum_{e \in \delta^+_G(v)} f(e) - $
\[ \sum_{\overrightarrow{e} \in \delta_G(v)} f(e). \]

Note that if \( f(e) \equiv 1 \pmod{k} \) for every edge \( e \), an \( f \)-weighted \( \beta \)-orientation is precisely a \( \beta \)-orientation.

An immediate observation is that if we wish to have a general result of the form of Theorem 6 for weighted orientations, it is necessary to assume that \( 2k + 1 \) is a prime number. For instance, take \( G \) to consist of two vertices \( u, v \) with an arbitrary number of edges between \( u \) and \( v \), consider a non-trivial divisor \( p \) of \( 2k + 1 \), and ask for a \( p \)-weighted \( \mathbb{Z}_{2k+1} \)-orientation \( \overrightarrow{G} \) of \( G \) (here, \( p \) denotes the function that maps each edge to \( p \pmod{2k+1} \)). Note that for any orientation, \( \partial p(v) \) is in the subgroup of \( \mathbb{Z}_{2k+1} \) generated by \( p \), and this subgroup does not contain \( 1, -1 \pmod{2k+1} \). In particular, there is no \( p \)-weighted \( \mathbb{Z}_{2k+1} \)-orientation of \( G \) with boundary \( \beta \) satisfying \( \beta(u) \equiv -\beta(v) \equiv 1 \pmod{2k + 1} \).

In Section 4, we will prove that Corollary 5 easily implies a weighted counterpart of Theorem 6 as in the following theorem, but with a stronger requirement on the edge-connectivity. Theorem 7 itself will be deduced directly from Theorem 6.

**Theorem 7.** Let \( p \geq 3 \) be a prime number and let \( G = (V, E) \) be a \((6p-8)(p-1)\)-edge-connected graph. For any mapping \( f : E \to \mathbb{Z}_p \setminus \{0\} \) and any \( \mathbb{Z}_p \)-boundary \( \beta \), \( G \) has an \( f \)-weighted \( \beta \)-orientation.

Theorem 7 turns out to be equivalent to the following seemingly more general result. Assume that we are given a directed graph \( \overrightarrow{G} = (V, \overrightarrow{E}) \) and a \( \mathbb{Z}_p \)-boundary \( \beta \). A \( \mathbb{Z}_p \)-flow with boundary \( \beta \) in \( \overrightarrow{G} \) is a mapping \( f : \overrightarrow{E} \to \mathbb{Z}_p \) such that \( \partial f(v) \equiv \beta(v) \pmod{p} \) for every \( v \). In other words, \( f \) is a \( \mathbb{Z}_p \)-flow with boundary \( \beta \) in \( \overrightarrow{G} = (V, \overrightarrow{E}) \) if and only if \( \overrightarrow{G} \) is an \( f \)-weighted \( \beta \)-orientation of its underlying non-oriented graph \( G = (V, E) \), where \( f \) is extended from \( \overrightarrow{E} \) to \( E \) in the natural way (i.e. for each \( e \in E \), \( f(e) := f(\overleftarrow{e}) \)).

In the remainder of the paper we will say that a directed graph \( \overrightarrow{G} \) is \( t \)-edge-connected if its underlying non-oriented graph, denoted by \( G \), is \( t \)-edge-connected.

**Theorem 8.** Let \( p \geq 3 \) be a prime number and let \( \overrightarrow{G} = (V, \overrightarrow{E}) \) be a directed \((6p-8)(p-1)\)-edge-connected graph. For any arc \( \overrightarrow{e} \in \overrightarrow{E} \), let \( L(\overrightarrow{e}) \) be a pair of distinct elements of \( \mathbb{Z}_p \). Then for every \( \mathbb{Z}_p \)-boundary \( \beta \), \( \overrightarrow{G} \) has a \( \mathbb{Z}_p \)-flow \( f \) with boundary \( \beta \) such that for any \( \overrightarrow{e} \in \overrightarrow{E} \), \( f(\overrightarrow{e}) \in L(\overrightarrow{e}) \).
This result can be seen as a choosability version of Theorem 6 (the reader is referred to [6] for choosability versions of some classical results on flows). To see that Theorem 8 implies Theorem 7, simply fix an arbitrary orientation of \( G \) and set \( L(\vec{e}) = \{ f(e), -f(e) \} \) for each arc \( \vec{e} \). We now prove that Theorem 7 implies Theorem 8. We actually prove a slightly stronger statement (holding in \( \mathbb{Z}_{2k+1} \) for any integer \( k \geq 1 \)).

**Lemma 9.** Let \( k \geq 1 \) be an integer, and let \( \vec{G} = (V, \vec{E}) \) be a directed non-orientated graph such that the underlying non-oriented graph \( G \) has an \( f \)-weighted \( \beta \)-orientation for any mapping \( f : E \to \mathbb{Z}_{2k+1} \setminus \{0\} \) and any \( \mathbb{Z}_{2k+1} \)-boundary \( \beta \). For every arc \( \vec{e} \in \vec{E} \), let \( L(\vec{e}) \) be a pair of distinct elements of \( \mathbb{Z}_{2k+1} \). Then for every \( \mathbb{Z}_{2k+1} \)-boundary \( \beta \), \( \vec{G} \) has a \( \mathbb{Z}_{2k+1} \)-flow \( g \) with boundary \( \beta \) such that \( g(\vec{e}) \in L(\vec{e}) \) for every \( \vec{e} \).

**Proof.** Let \( \beta \) be a \( \mathbb{Z}_{2k+1} \)-boundary of \( \vec{G} \). Consider a single arc \( \vec{e} = (u, v) \) of \( \vec{G} \). Choosing one of the two values of \( L(\vec{e}) \), say \( a \) or \( b \), will either add \( a \) to \( \partial g(u) \) and subtract \( a \) from \( \partial g(v) \), or add \( b \) to \( \partial g(u) \) and subtract \( b \) from \( \partial g(v) \). Note that 2 and \( 2k + 1 \) are relatively prime, so the element \( 2^{-1} \) is well-defined in \( \mathbb{Z}_{2k+1} \). If we now add \( 2^{-1}(a + b) \) to \( \beta(v) \) and subtract \( 2^{-1}(a + b) \) from \( \beta(u) \), the earlier choice is equivalent to choosing between the two following options: adding \( 2^{-1}(a - b) \) to \( \partial g(u) \) and subtracting \( 2^{-1}(a - b) \) from \( \partial g(v) \), or adding \( 2^{-1}(b - a) \) to \( \partial g(u) \) and subtracting \( 2^{-1}(b - a) \) from \( \partial g(v) \). This is equivalent to choosing an orientation for an edge of weight \( 2^{-1}(a - b) \). It follows that finding a \( \mathbb{Z}_{2k+1} \)-flow \( g \) with boundary \( \beta \) such that for any \( \vec{e} \in \vec{E} \), \( g(\vec{e}) \in L(\vec{e}) \) is equivalent to finding an \( f \)-weighted \( \beta' \)-orientation for some other \( \mathbb{Z}_{2k+1} \)-boundary \( \beta' \) of \( G \), where the weight \( f(e) \) of each edge \( e \) is \( 2^{-1} \) times the difference between the two elements of \( L(\vec{e}) \). \( \square \)

We now consider the case where \( L(\vec{e}) = \{0, 1\} \) for every arc \( \vec{e} \in \vec{E} \). Let \( f_{2^{-1}} : \vec{E} \to \mathbb{Z}_{2k+1} \) denote the function that maps each arc \( \vec{e} \) to \( 2^{-1} \) (mod \( 2k + 1 \)). The same argument as in the proof of Lemma 9 implies that if \( G \) has an \( f_{2^{-1}} \)-weighted \( \beta \)-orientation for every \( \mathbb{Z}_{2k+1} \)-boundary \( \beta \), then for every \( \mathbb{Z}_{2k+1} \)-boundary \( \beta \), the digraph \( \vec{G} \) has a \( \mathbb{Z}_{2k+1} \)-flow \( f \) with boundary \( \beta \) such that \( f(\vec{e}) \in L(\vec{e}) \) for every \( \vec{e} \).

The following is a simple corollary of Theorem 6.

**Corollary 10.** Let \( \ell \geq 1 \) be an odd integer and let \( k \geq 1 \) be relatively prime with \( \ell \). Let \( G = (V, E) \) be a \( (3\ell - 3) \)-edge-connected graph, and let \( k : E \to \mathbb{Z}_\ell \) be the mapping that assigns \( k \) (mod \( \ell \)) to each edge \( e \in E \). Then for any \( \mathbb{Z}_\ell \)-boundary \( \beta \), \( G \) has a \( k \)-weighted \( \beta \)-orientation.
Proof. Observe that $\beta' = k^{-1} \cdot \beta$ is a $\mathbb{Z}_k$-boundary ($k^{-1}$ is well defined in $\mathbb{Z}_k$). It follows from Theorem 6 that $G$ has a $\beta'$-orientation. Note that this corresponds to a $k$-weighted $\beta$-orientation of $G$, as desired. □

As a consequence, the following is an equivalent version of Theorem 6 (see also [12, 14]).

**Theorem 11.** Let $k \geq 1$ be an integer and let $\vec{G} = (V, \vec{E})$ be a directed $6k$-edge-connected graph. Then for every $\mathbb{Z}_{2k+1}$-boundary $\beta$, $\vec{G}$ has a $\mathbb{Z}_{2k+1}$-flow $f$ with boundary $\beta$ such that $f(\vec{E}) \in \{0, 1\}$ (mod $2k + 1$).

This version of Theorem 6 will allow us to derive interesting results on antisymmetric flows in directed highly edge-connected graphs. Given an abelian group $(B, +)$, a $B$-flow in $\vec{G}$ is a mapping $f : \vec{E} \to B$ such that $\partial f(v) = 0$ for every vertex $v$, where all operations are performed in $B$. A $B$-flow $f$ in $\vec{G} = (V, \vec{E})$ is a nowhere-zero $B$-flow (or a $B$-NZF) if $0 \not\in f(\vec{E})$, i.e., each arc of $\vec{G}$ is assigned a non-zero element of $B$. If no two arcs receive inverse elements of $B$, then $f$ is an antisymmetric $B$-flow (or a $B$-ASF).

Since $0 = -0$, a $B$-ASF is also a $B$-NZF. It was conjectured by Tutte that every directed 2-edge-connected graph has a $\mathbb{Z}_5$-NZF [21], and that every directed 4-edge-connected graph has a $\mathbb{Z}_3$-NZF (see [18] and [3]). Antisymmetric flows were introduced by Nešetřil and Raspau in [16]. A natural obstruction for the existence of an antisymmetric flow in a directed graph $\vec{G}$ is the presence of directed 2-edge-cut in $\vec{G}$. Nešetřil and Raspau asked whether any directed graph without directed 2-edge-cut has a $B$-ASF, for some $B$. This was proved by DeVos, Johnson, and Seymour in [7], who showed that any directed graph without directed 2-edge-cut has a $\mathbb{Z}_8^4 \times \mathbb{Z}_3^7$-ASF. It was later proved by DeVos, Nešetřil, and Raspau [8], that the group could be replaced by $\mathbb{Z}_2^8 \times \mathbb{Z}_3^9$. The best known result is due to Dvořák, Kaiser, Král’, and Sereni [10], who showed that any directed graph without directed 2-edge-cut has a $\mathbb{Z}_2^2 \times \mathbb{Z}_3^9$-ASF (this group has 157464 elements).

Adding a stronger condition on the edge-connectivity allows to prove stronger results on the size of the group $B$. It was proved by DeVos, Nešetřil, and Raspau [8], that every directed 4-edge-connected graph has a $\mathbb{Z}_2^4 \times \mathbb{Z}_3^4$-ASF, that every directed 5-edge-connected graph has a $\mathbb{Z}_3^5$-ASF, and that every directed 6-edge-connected graph has a $\mathbb{Z}_2 \times \mathbb{Z}_3^2$-ASF.
In [11], Jaeger conjectured the following weaker version of Tutte’s 3-flow conjecture: \textit{there is a constant }k\textit{ such that every }k\text{-edge-connected graph has a }\mathbb{Z}_3\text{-NZF.} This conjecture was recently solved by Thomassen [19], who proved that every 8-edge-connected graph has a \(\mathbb{Z}_3\)-NZF, and was improved by Lovász, Thomassen, Wu and Zhang [15], that every 6-edge-connected graph has a \(\mathbb{Z}_3\)-NZF (this is a simple consequence of Theorem 6).

The natural antisymmetric variant of Jaeger’s weak 3-flow conjecture would be the following: \textit{there is a constant }k\textit{ such that every directed }k\text{-edge-connected graph has a }\mathbb{Z}_5\text{-ASF}.

Note that the size of the group would be best possible, since in \(\mathbb{Z}_2\) and \(\mathbb{Z}_2 \times \mathbb{Z}_2\) every element is its own inverse, while a \(\mathbb{Z}_3\)-ASF or a \(\mathbb{Z}_4\)-ASF has to assign the same value to all the arcs (and this is impossible in the digraph on two vertices \(u, v\) with exactly \(k\) arcs directed from \(u\) to \(v\), for any integer \(k \equiv 1 \pmod{12}\)).

Our final result is the following.

\textbf{Theorem 12.} For any \(k \geq 2\), every directed \(\lceil \frac{6k}{k-1} \rceil\)-edge-connected graph has a \(\mathbb{Z}_{2k+1}\)-ASF.

\textit{Proof.} Let \(k \geq 2\), and let \(\vec{G}\) be a directed \(\lceil \frac{6k}{k-1} \rceil\)-edge-connected graph. Let \(\vec{H}\) be the directed graph obtained from \(\vec{G}\) by replacing every arc \(\vec{e}\) by \(k - 1\) arcs with the same tail and head as \(\vec{e}\), and let \(H\) be the non-oriented graph underlying \(\vec{H}\). Let \(\beta(v) = d^-_G(v) - d^+_G(v)\) for every \(v\). Since \(\vec{G}\) is \(\lceil \frac{6k}{k-1} \rceil\)-edge-connected, \(H\) is \(6k\)-edge-connected and by Theorem 11, \(\vec{H}\) has a \(\mathbb{Z}_{2k+1}\)-flow \(f\) with boundary \(\beta\) with flow values in the set \(\{0, 1\} \pmod{2k+1}\). For any arc \(\vec{e}\) of \(\vec{G}\), let \(g(\vec{e})\) be the sum of the values of the flow \(f\) on the \(t\) arcs corresponding to \(\vec{e}\) in \(\vec{H}\). Then \(g\) is a \(\mathbb{Z}_{2k+1}\)-flow with boundary \(\beta\) in \(\vec{G}\), with flow values in the set \(\{0, 1, \ldots, k-1\} \pmod{2k+1}\). Now, set \(g'(\vec{e}) = g(\vec{e}) + 1\) for every arc \(\vec{e}\). Hence every \(\vec{e}\) is assigned a value in \(\{1, \ldots, k\} \pmod{2k+1}\), and \(\partial g'(v) \equiv \partial g(v) + d^+_G(v) - d^-_G(v) \equiv \beta'(v) + d^+_G(v) - d^-_G(v) \equiv 0 \pmod{2k+1}\) for every \(v\). Thus \(g'\) is a \(\mathbb{Z}_{2k+1}\)-flow of \(\vec{G}\) with flow values in the set \(\{1, \ldots, k\} \pmod{2k+1}\), and thus a \(\mathbb{Z}_{2k+1}\)-ASF in \(\vec{G}\), as desired. This concludes the proof of Theorem 12. \(\square\)

As a corollary, we directly obtain:

\textbf{Corollary 13.}

(i) \textit{Every directed }7\text{-edge-connected graph has a }\mathbb{Z}_{15}\text{-ASF.}
(ii) Every directed 8-edge-connected graph has a $\mathbb{Z}_9$-ASF.
(iii) Every directed 9-edge-connected graph has a $\mathbb{Z}_7$-ASF.
(iv) Every directed 12-edge-connected graph has a $\mathbb{Z}_5$-ASF.

By duality, using the results of Nešetřil and Raspaud [16], Corollary 13 (which, again, can be seen as an antisymmetric analogue of the statement of Jaeger’s conjecture) directly implies that every orientation of a planar graph of girth (length of a shortest cycle) at least 12 has a homomorphism to an oriented graph on at most 5 vertices. This was proved by Borodin, Ivanova and Kostochka in 2007 [4], and it is not known whether the same holds for planar graphs of girth at least 11. On the other hand, it was proved by Nešetřil, Raspaud and Sopena [17] that there are orientations of some planar graphs of girth at least 7 that have no homomorphism to an oriented graph of at most 5 vertices. By duality again, this implies that there are directed 7-edge-connected graphs with no $\mathbb{Z}_5$-ASF. We conjecture the following:

**Conjecture 14.** Every directed 8-edge-connected graph has a $\mathbb{Z}_5$-ASF.

It was conjectured by Lai [13] that for every $k \geq 1$, every $(4k + 1)$-edge-connected graph $G$ has a $\beta$-orientation for every $\mathbb{Z}_{2k+1}$-boundary $\beta$ of $G$. If true, this conjecture would directly imply (using the same proof as that of Theorem 12) that for any $k \geq 2$, every directed $\left\lceil \frac{4k+1}{k-1} \right\rceil$-edge-connected graph has a $\mathbb{Z}_{2k+1}$-ASF. In particular, this would show that directed 5-edge-connected graph have a $\mathbb{Z}_{13}$-ASF, directed 6-edge-connected graph have a $\mathbb{Z}_9$-ASF, directed 7-edge-connected graph have a $\mathbb{Z}_7$-ASF, and directed 9-edge-connected graph have a $\mathbb{Z}_5$-ASF. The bound on directed 5-edge-connected graph would also directly imply, using the proof of the main result of [10], that directed graphs with no directed 2-edge-cut have a $\mathbb{Z}_2^2 \times \mathbb{Z}_3^4 \times \mathbb{Z}_{13}$-ASF.

3. Proof of Theorem 3

We first recall the following (weak form of a) classical result by Mader (see [9], Theorem 1.4.3):

**Lemma 15.** Given an integer $k \geq 1$, if $G = (V, E)$ is a graph with average degree at least $4k$, then there is a subset $X$ of $V$ such that $|X| > 1$ and $G[X]$ is $(k + 1)$-edge-connected.

We will also need the following result of Thomassen [20], which is a simple consequence of Theorem 6.
Theorem 16 ([20]). Let \( k \geq 3 \) be an odd integer, \( G = (V_1, V_2, E) \) be a bipartite graph, and \( f : V_1 \cup V_2 \to \mathbb{Z}_k \) be a mapping satisfying 
\[
\sum_{v \in V_1} f(v) \equiv \sum_{v \in V_2} f(v) \pmod{k}.
\]
If \( G \) is \((3k - 3)\)-edge-connected, then \( G \) has a spanning subgraph \( H \) such that for any \( v \in V \), \( d_H(v) \equiv f(v) \pmod{k} \).

Let \( G \) be a graph, and let \( X \) and \( Y \) be two disjoint subsets of vertices of \( G \). The set of edges of \( G \) with one endpoint in \( X \) and the other in \( Y \) is denoted by \( E(X, Y) \).

We are now ready to prove Theorem 3.

Proof of Theorem 3. We proceed by induction on \( n \). For \( n = 1 \), this is a direct consequence of Theorem 1, so suppose that \( n \geq 2 \). Each basis \( B_s \) can be considered as an \( n \times n \) matrix where each column is a vector with support of size at most 2. Let \( B = \biguplus_{i=1}^{t} B_i \).

For \( 1 \leq i \leq n \), a vector is called an \( i \)-vector if its support is the singleton \( \{i\} \) (in other words, the \( i \)-th entry is non-zero and all the other entries are zero). Suppose that for some \( 1 \leq i \leq n \), \( B \) contains at least \( p - 1 \) \( i \)-vectors. Let \( C \) be the set of \( i \)-vectors of \( B \). Clearly, each basis contains at most one \( i \)-vector. For every \( B_s \), let \( B'_s \) be the matrix obtained from \( B_s \) by removing its \( i \)-vector (if any) and the \( i \)th row. Clearly \( B'_s \) is or contains a basis of \( \mathbb{Z}_{p}^{n-1} \). By induction hypothesis, \( \biguplus_{s=1}^{t} B'_s \) forms an additive basis of \( \mathbb{Z}_{p}^{n-1} \). In other words, for any vector \( \beta = (\beta_1, ..., \beta_i, ..., \beta_n) \in \mathbb{Z}_{p}^n \), there is a subset \( Y_1 \) of \( B \setminus C \) which sums to \((\beta_1, ..., \hat{\beta}_i, ..., \beta_n)\) for some \( \hat{\beta}_i \). Since \( |C| \geq p - 1 \), it follows from Theorem 1 that there is a subset \( Y_2 \) of \( C \) which sums to \((0, ..., \beta_i - \hat{\beta}_i, ..., 0) \). Hence \( Y_1 \cup Y_2 \) sums to \( \beta \).

Thus we can suppose that there are at most \( p - 2 \) \( i \)-vectors for every \( i \). Then there are at least \( 8(3p - 4)n \) vectors with a support of size 2 in \( B \). Since there are at most \( \ell \) distinct shadows of size 2 in \( B \), there are at least \( 8(3p - 4)n \) vectors with the same (unordered) shadow of size 2, say \( \{a_1, a_2\} \) (recall that shadows are multisets, so \( a_1 \) and \( a_2 \) might coincide).

Let \( G \) be the graph (recall that graphs in this paper are allowed to have multiple edges) with vertex set \( V = \{v_1, ..., v_n\} \) and edge set \( E \), where edges \( v_i v_j \) are in one-to-one correspondence with vectors of \( B \) with support \( \{i, j\} \) and shadow \( \{a_1, a_2\} \). Then \( G \) contains at least \( 8(3p - 4)n \) edges.

We now consider a random partition of \( V \) into 2 sets \( V_1, V_2 \) (by assigning each vertex of \( V \) uniformly at random to one of the sets \( V_k \),
that there is a set $V_k$ such that $G \subseteq X$ and $i$ the elements of the vector of $B$ corresponding with $e$ has entry $a_1$ (resp. $a_2$) at the index associated to the endpoint of $e$ in $V_1$ (resp. $V_2$).

Since the graph $G' = (V, E')$ has average degree at least $4(3p - 4)$, it follows from Lemma 15 that there is a set $X \subseteq V$ of at least 2 vertices, such that $G'[X]$ is $(3p - 3)$-edge-connected. Set $H = G'[X]$ and $F$ the edge set of $H$. Note that $H$ is bipartite with bipartition $X_1 = X \cap V_1$ and $X_2 = X \cap V_2$.

For each integer $1 \leq s \leq t$, let $B_s^*$ be the matrix obtained from $B_s$ by doing the following: for each vertex $v_i$ in $X_1$ (resp. $X_2$), we multiply all the elements of the $i$th row of $B_s$ by $a_1^{-1}$ (resp. $a_2^{-1}$), noting that all the operations are performed in $\mathbb{Z}_p$. Let $B^* = \bigcup_{s=1}^t B_s^*$. Note that each vector of $B^*$ corresponding to some edge $e \in F$ has shadow $\{1, -1\}$ ($1$ is the entry indexed by the endpoint of $e$ in $X_1$ and $-1$ is the entry indexed by the endpoint of $e$ in $X_2$). It is easy to verify the following.

- Each $B_s^*$ is a linear basis of $\mathbb{Z}_p^n$.
- $B^*$ is an additive basis if and only if $B^*$ is an additive basis.

Hence it suffices to prove that $B^*$ is an additive basis.

Without loss of generality, suppose that $X = \{v_m, ..., v_n\}$ for some $m \leq n - 1$. By contracting $k$ rows of a matrix, we mean deleting these $k$ rows and adding a new row consisting of the sum of the $k$ rows. For each $1 \leq s \leq t$, let $B_s'$ be the matrix of $m$ rows obtained from $B_s^*$ by contracting all $m^{th}$, $(m + 1)^{th}$, ..., $n^{th}$ rows. Note that the operation of contracting $k$ rows decreases the rank of the matrix by at most $k - 1$ (since it is the same as replacing one of the rows by the sum of the $k$ rows, which preserves the rank, and then deleting the $k - 1$ other rows). Let $B' = \bigcup_{s=1}^t B_s'$. Since each $B_s'$ is a linear basis of $\mathbb{Z}_p^n$, each $B_s'$ has rank at least $m$ and therefore contains a basis of $\mathbb{Z}_p^m$. Hence, by induction hypothesis, $B' \setminus B_0'$ is an additive basis of $\mathbb{Z}_p^m$, where $B_0'$ is the set of all columns with empty support in $B'$. For every $\beta = (\beta_1, ..., \beta_n) \in \mathbb{Z}_p^n$, let $\beta' = (\beta_1, ..., \beta_{m-1}, \sum_{i=m}^n \beta_i) \in \mathbb{Z}_p^m$. Then there is a subset $Y'$ of $B' \setminus B_0'$ which sums to $\beta'$. Let $Y^*$ and $B_0^*$ be the subsets of $B^*$ corresponding to $Y'$ and $B_0'$, respectively. Then $Y^*$
that there is a subset $\beta = (\beta_1, \ldots, \beta_{m-1}, \hat{\beta}_m, \ldots, \hat{\beta}_n)$, where $\sum_{i=1}^{n} \beta_i \equiv \sum_{i=1}^{m} \hat{\beta}_i \pmod{p}$.

Recall that for each edge $e \in F$, the corresponding vector in $B^*$ has precisely two non-zero entries, $(1, -1)$, each with index in $X$. Hence the vector corresponding to each $e \in F$ in $B'$ has empty support. Thus the set of vectors in $B^*$ corresponding to the edge set $F$ is a subset of $B_0^*$, which is disjoint from $Y$.

For each $v_i \in X_1$, let $\beta_X(v_i) = \beta_i - \hat{\beta}_i$, and for each $v_i \in X_2$, let $\beta_X(v_i) = \hat{\beta}_i - \beta_i$. Since $\sum_{i=1}^{n} \beta_i \equiv \sum_{i=1}^{m} \hat{\beta}_i \pmod{p}$, we have $\sum_{v_i \in X \cap V_1} \beta_X(v_i) = \sum_{v_i \in X \cap V_2} \beta_X(v_i)$. Since $H$ is $(3p - 3)$-edge-connected, it follows from Theorem 16 that there is a subset $F' \subseteq F$ such that, in the graph $(X, F')$, each vertex $v_i \in X_1$ has degree $\beta_i - \hat{\beta}_i \pmod{p}$ and each vertex $v_i \in X_2$ has degree $\hat{\beta}_i - \beta_i \pmod{p}$. Therefore, $F'$ corresponds to a subset $Z^*$ of vectors of $B_0^*$, summing to $(0, \ldots, 0, \beta_m - \hat{\beta}_m, \ldots, \beta_n - \hat{\beta}_n)$. Then $Y^* \cup Z^*$ sums to $\beta$. It follows that $B^*$ is an additive basis of $\mathbb{Z}_p^n$, and so is $B$. This completes the proof.

4. TWO PROOFS OF (VERSIONS OF) THEOREM 7

We now give two proofs of (versions of) Theorem 7. The first one is a direct application of Corollary 5, but requires a stronger assumption on the edge-connectivity of $G$ ($24p^2 - 54p + 28$ instead of $6p^2 - 14p + 8$ for the second proof).

First proof of Theorem 7. We fix some arbitrary orientation $\tilde{G} = (V, \tilde{E})$ of $G$ and denote the vertices of $G$ by $v_1, \ldots, v_n$. The number of edges of $G$ is denoted by $m$. For each arc $\tilde{e} = (v_i, v_j)$ of $\tilde{G}$, we associate $\tilde{e}$ to a vector $x_\tilde{e} \in (\mathbb{Z}_p^n)_0$ in which the $i^{th}$-entry is equal to $f(e) \pmod{p}$, the $j^{th}$-entry is equal to $-f(e) \pmod{p}$ and all the remaining entries are equal to 0 (mod $p$).

Let us consider the following statements.

1. For each $\mathbb{Z}_p$-boundary $\beta$, there is an $f$-weighted $\beta$-orientation of $G$.
2. For each $\mathbb{Z}_p$-boundary $\beta$ there is a vector $(a_e)_{e \in E} \in \{-1, 1\}^m$, such that $\sum_{e \in E} a_e x_\tilde{e} \equiv \beta \pmod{p}$.
3. For each $\mathbb{Z}_p$-boundary $\beta$ there is a vector $(a_e)_{e \in E} \in \{0, 1\}^m$ such that $\sum_{e \in E} 2a_e x_\tilde{e} \equiv \beta \pmod{p}$.

Clearly, (a) is equivalent to (b). We now claim that (b) is equivalent to (c). To see this, simply do the following for each arc $\tilde{e} = (v_i, v_j)$ of
$G$: add $f(e)$ to the $j$th-entry of $x_e$ and to $\beta(v_j)$, and subtract $f(e)$ from the $i$th-entry of $x_e$ and from $\beta(v_i)$. To deduce $c$ from Corollary 5, what is left is to show that $\{a_e : e \in E\}$ can be decomposed into sufficiently many linear bases of $(\mathbb{Z}_p^n)_0$. This follows from the fact that $G$ is $(8(p-1)(3p-4)+2p-4)$-edge-connected (and therefore contains $4(p-1)(3p-4)+p-2$ edge-disjoint spanning trees) and that the set of vectors $a_e$ corresponding to the edges of a spanning tree of $G$ forms a linear basis of $(\mathbb{Z}_p^n)_0$ (see [12]).

A second proof consists in mimicking the proof of Theorem 3 (it turns out to give a better bound for the edge-connectivity of $G$).

Second proof of Theorem 7. As before, all values and operations are considered modulo $p$. We can assume without loss of generality that $f(E) \in \{1, 2, \ldots, \frac{p-1}{2}\}$, since otherwise we can replace the value $f(e)$ of an edge $e$ by $-f(e)$, without changing the problem.

We prove the result by induction on the number of vertices of $G$. The result is trivial if $G$ contains only one vertex, so assume that $G$ has at least two vertices.

For any $1 \leq i \leq k$, let $E_i$ be the set of edges $e \in E$ with $f(e) = i$, and let $G_i = (V, E_i)$. Since $G$ is $(6p-8)(p-1)$-edge-connected, $G$ has minimum degree at least $(6p-8)(p-1)$ and then average degree at least $(6p-8)(p-1)$. As a consequence, there exists $i$ such that $G_i$ has average degree at least $12p-16$. By Lemma 15, since $\frac{12p-16}{4}+1 = 3p-3$, $G_i$ has an induced subgraph $H = (X, F)$ with at least two vertices such that $H$ is $(3p-3)$-edge-connected. Let $G/X$ be the graph obtained from $G$ by contracting $X$ into a single vertex $x$ (and removing possible loops). Since $H$ contains more than one vertex, $G/X$ has less vertices than $G$ (note that possibly, $X = V$ and in this case $G/X$ consists of the single vertex $x$). Since $G$ is $(6p-8)(p-1)$-edge-connected, $G/X$ is also $(6p-8)(p-1)$-edge-connected. Hence by the induction hypothesis it has an $f$-weighted $\beta$-orientation, where we consider the restriction of $f$ to the edge-set of $G/X$, and we define $\beta(x) = \beta(X)$. Note that this orientation corresponds to an orientation of all the edges of $G$ with at most one endpoint in $X$.

We now orient arbitrarily the edges of $G[X]$ not in $F$ (the edge-set of $H$), and update the values of the $\mathbb{Z}_p$-boundary $\beta$ accordingly (i.e. for each $v \in X$, we subtract from $\beta(v)$ the contribution of the arcs that were already oriented). It is easy to see that as the original $\beta$ was a boundary, the new $\beta$ is indeed a boundary. Finally, since all the edges of $H$ have the same weight, and since $H$ is $(3p-3)$-edge-connected,
it follows from Corollary 10 that $H$ has an $f$-weighted $\beta$-orientation (with respect to the updated boundary $\beta$). The orientations combine into an $f$-weighted $\beta$-orientation of $G$, as desired. □

ACKNOWLEDGMENTS

We would like to thank the referees for their suggestions and for mentioning the existence of the unpublished manuscript [14].

REFERENCES

[1] N. Alon, N. Linial and R. Meshulam Additive bases of vector spaces over prime fields, J. Combin. Theory Ser. A 57 (1991), 203–210.
[2] N. Alon, M. Nathanson, and I. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56(2) (1996), 404–417.
[3] J.A. Bondy and U.S.R. Murty, Graph Theory with Applications, Macmillan, London and Elsevier, New York, 1976.
[4] O.V. Borodin, A.O. Ivanova and A.V. Kostochka, Oriented 5-coloring of sparse plane graphs, J. Applied and Industrial Math. 1(1) (2007), 9–17.
[5] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935), 30–32.
[6] M. DeVos, Matrix choosability, J. Combin. Theory Ser. A 90 (2000), 197–209.
[7] M. DeVos, T. Johnson, and P. Seymour, Cut coloring and circuit covering, Manuscript.
[8] M. DeVos, J. Nešetřil, and A. Raspaud, Antisymmetric flows and edge-connectivity, Discrete Math. 276(13) (2004), 161–167.
[9] R. Diestel, Graph Theory, Graduate Texts in Mathematics, Springer (2005).
[10] Z. Dvořák, T. Kaiser, D. Kráľ, and J.-S. Sereni, A note on antisymmetric flows in graphs, European J. Combin. 31 (2010), 320–324.
[11] F. Jaeger, Flows and generalized coloring theorems in graphs, J. Combin. Theory Ser. B 26 (1979), 205–216.
[12] F. Jaeger, N. Linial, C. Payan, and M. Tarsi, Group connectivity of graphs – A non homomogeneous analogue of nowhere-zero flow properties, J. Combin. Theory Ser. B 56 (1992), 165–182.
[13] H.-J. Lai, Mod $(2p + 1)$-orientations and $K_{1,2p+1}$-decompositions, SIAM J. Discrete Math. 21 (2007), 844–850.
[14] H.-J. Lai and P. Li, Additive bases and strongly $\mathbb{Z}_{2s+1}$-connectedness, Manuscript.
[15] L.M. Lovász, C. Thomassen, Y. Wu, and C.-Q. Zhang, Nowhere-zero 3-flows and modulo k-orientations, J. Combin. Theory Ser.B 103 (2013), 587–598.
[16] J. Nešetřil and A. Raspaud, Antisymmetric flows and strong colourings of oriented graphs, Ann. Inst. Fourier 49(3) (1999), 1037–1056.
[17] J. Nešetřil, A. Raspaud and E. Sopena, Colorings and girth of oriented planar graphs, Discrete Math. 165–166 (1997), 519–530.
[18] R. Steinberg, Grötzsch’s Theorem dualized, M. Math Thesis, University of Waterloo, 1976.
[19] C. Thomassen, The weak 3-flow conjecture and the weak circular flow conjecture, J. Combin. Theory Ser. B 102 (2012), 521–529.
[20] C. Thomassen, Graph factors modulo k, J. Combin. Theory Ser. B 106 (2014), 174–177.
[21] W.T. Tutte, A Contribution on the Theory of Chromatic Polynomial, Canad. J. Math. 6 (1954), 80–91.
[22] W.T. Tutte, On the algebraic theory of graph colorings, J. Combin. Theory 1 (1966), 15–50.