GRASSMANN HOMOMORPHISM AND HAJÓS-TYPE THEOREMS

TOMMY R. JENSEN

Abstract.

Let V and W be vector spaces over a common field, and let $\mathcal{S}$ and $\mathcal{T}$ be sets of subspaces of V and W, respectively. A linear function $\varphi : V \to W$ is called a (Grassmann) homomorphism from $\mathcal{S}$ to $\mathcal{T}$ if $\varphi(S) \in \mathcal{T}$ holds for every $S \in \mathcal{S}$.

Coloring of graphs and hypergraphs and flows in graphs can be reformulated in terms of these homomorphisms.

The main results are constructive characterizations of the sets $\mathcal{S}$ of lines for which there is no homomorphism from $\mathcal{S}$ to a singleton set $\mathcal{T}$ with a line as its element.

Keywords: Hajós Construction; finite Grassmannian; homomorphism; combinatorics; complexity classes; graph theory.

MSC2010 classification: 20G40, 14M15, 05C15, 03D15.

1. Introduction

The Hajós Theorem [3] in Graph Theory states that for every natural number k, if a graph is not colorable with fewer than k colors, then it contains a subgraph obtained from K_k by recursively

(i) identifying two non-adjacent vertices, or
(ii) from two disjoint graphs G_1 and G_2 already obtained, in which G_1 has an edge x_1y_1 and G_2 has an edge x_2y_2, first deleting x_1y_1 and x_2y_2, then identifying x_1 with x_2, and finally adding the edge y_1y_2.

The construction in (ii) was also studied earlier by Dirac [1], and it is sometimes referred to as the 'Dirac-Hajós Construction'. Applications of the Hajós Construction include the proof of existence of 4-regular planar 4-critical graphs by Koester [9], and constructions by Liu and Zhang [11] of examples of triangle-free 4-critical graphs for which the decision problem of their 3-colorability tends to be particularly hard to solve for traditional backtracking algorithms.

The Hajós Theorem is also interesting for its connections to computational complexity. Mansfield and Welsh [13] noted that if for any $k > 2$ there exists a polynomial P for which every graph of chromatic number k and order n contains a subgraph that can be so constructed that operations (i) and (ii) are used a total of at most $P(n)$ times, then the two complexity classes NP and co-NP coincide.

Pitassi and Urquhart [17] studied a restricted version of the Hajós construction in which operation (ii) is replaced by

(ii)' taking the intersection of two graphs G_1 and G_2 already obtained, for which $V(G_1) = V(G_2)$, and for which there are edges x_1y of G_1 and x_2y of

G_2 such that $E(G_1) \setminus E(G_2) = \{x_1y\}$ and $E(G_2) \setminus E(G_1) = \{x_2y\}$, and $x_1x_2 \in E(G_1 \cap G_2)$.

They proved that the complexity of this construction is closely related to the complexity of proofs in extended Frege Systems studied in logic. While restrictive compared to (ii), in the sense that (ii)' may only be performed on very particular pairs G_1, G_2 of graphs, the operations (i) and (ii)' remain sufficient to construct from K_k every graph of chromatic number at least k. This variation of the Hajós construction has been restricted further for the case $k = 4$ by Iwama, Seto and Tamaki [5], who described a construction of 4-chromatic planar graphs starting from K_4 that replaces operations (i) and (ii)' by operations that preserve planarity, so that every intermediate graph of the construction remains planar and 4-chromatic. They showed that the complexity of their construction is polynomially equivalent to the classical construction.

A graph is *critical k-chromatic* or *k-critical,* if it is k-chromatic and every proper subgraph is $(k-1)$-colorable. Hajós asked whether the Hajós construction of any k-critical graph may be so restricted that only k-critical graphs appear in the intermediate steps. A negative answer to this question was obtained by Hanson, Robinson and Toft [4] in the case $k \geq 8$, and by Jensen and Royle [7] for $4 \leq k \leq 7$. Tutte [20] announced a variation of the Hajós construction that involves a condition of criticality of only some of the intermediate graphs. From this version he was able to deduce Brooks' Theorem.

Even though there are several known variations of the Hajós construction, each capable of constructing any k-chromatic graph, it seems difficult to apply any of them in proofs of known structural results about these graphs, let alone in proofs of new results. Ore [15] introduced a more restrictive variation of the Hajós Construction, aiming to apply it to proofs of structure theorems for graphs with a given chromatic number, though he provided no example of such a proof. Tutte's version mentioned above may possibly be the only example with some small success in this direction. The reason for lack of progress seems to be the difficulty to gain enough control of the structure of intermediate graphs.

We will consider to move also in the opposite direction; by removing some restrictions, without introducing any steps that may reduce chromatic number, we allow a richer selection of possible construction steps. This should be expected to reduce the number of steps to produce a given graph G, which seems useful in a complexity study. Dirac [1] already studied a more general version of step (ii) as a tool to construct critical graphs. Jaeger [6] provided a generalization of the Hajós Theorem to representable matroids. In the language of matroids represented over a field, the chromatic number is replaced by a corresponding 'critical exponent', defined in terms of evaluations of the Tutte polynomial of the matroid, see also Oxley [16]. The generalization to representable matroids means that there exists a 'Hajós-type' construction also of graphs that do not allow a 'nowhere-zero k-flow' (see Chapter 2 for the definition).

Other variations of the Hajós Theorem have also been obtained. A Hajós-type theorem for list coloring has been introduced by Gravier [2] and refined by Král [10]. Another Hajós-type theorem for graph homomorphism is due to Nešetřil [14]. Two versions for circular coloring were presented by Zhu [21, 22]. In this paper we

do not address these variations further, since they are not naturally expressible in our setting.

The plan for this paper is to formulate and study a homomorphism concept that provides a common generalization of Graph Coloring, Hypergraph Coloring and Nowhere-Zero Flow. The notation and terminology are introduced in Section 2, Section 3 establishes that coloring and flow problems for graphs are indeed special cases of this concept and it addresses computational complexity issues. Section 4 contains three theorems that have a similar role as the Hajós Theorem and its variations for Graph Coloring. Theorem 1 deals with a very restrictive construction for which there is no direct counterpart for constructing graphs of a given chromatic number. Theorem 2 deals with a less restrictive construction corresponding to (i) and (ii)' mentioned above. Theorem 3 is the least restrictive, with constructions steps that are similar to (i) and (ii). The latter theorem is closely related to Jaeger's theorem on representable matroids; however, the details of this relationship fall outside the scope of this paper.

2. Notation and Terminology

Let $\mathbb{F}$ be any field. In the following, all vector spaces are finite dimensional vector spaces over $\mathbb{F}$. Let V be such a vector space. For a natural number d the set of all d-dimensional subspaces of V is the *Grassmannian* $\mathrm{Gr}(d, V)$. The set of all subspaces of V will be denoted by $\mathrm{Gr}(V)$, hence

$$\mathrm{Gr}(V) = \bigcup_{d=0}^{\dim(V)} \mathrm{Gr}(d, V).$$

The subset $\mathrm{Gr}^*(V)$ contains all subspaces of positive dimension; $\mathrm{Gr}^*(V) = \mathrm{Gr}(V) \setminus \mathrm{Gr}(0, V)$. The 0-dimensional subspace of V is *trivial*, and the elements of $\mathrm{Gr}(1, V)$ are *lines*.

If $v_1, v_2, \ldots, v_n$ are any elements of a vector space, then $\langle v_1, v_2, \ldots, v_n \rangle$ denotes the subspace in which the elements are all linear combinations $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ with $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$.

When V and W are vector spaces, we let $\mathcal{L}(V, W)$ denote the set of all linear functions from V to W. Also $\mathcal{L}(V, W)$ naturally forms a vector space over $\mathbb{F}$.

For $\varphi \in \mathcal{L}(V, W)$ and $S \subseteq \mathrm{Gr}(V)$ a set of subspaces of V, the *image of S under φ* is the set

$$\varphi(S) = \{\varphi(X) : X \in S\},$$

where $\varphi(X) = \{\varphi(v) : v \in X\} \in \mathrm{Gr}(W)$. In particular $S \subseteq \mathrm{Gr}(V)$ implies $\varphi(S) \subseteq \mathrm{Gr}(W)$. In the following φ is considered as a function from the set of subsets of $\mathrm{Gr}(V)$ to the set of subsets of $\mathrm{Gr}(W)$ in this natural sense.

Definition 1 Let $\mathcal{S} \subseteq \mathrm{Gr}(V)$ and $\mathcal{T} \subseteq \mathrm{Gr}(W)$. A function $\varphi \in \mathcal{L}(V, W)$ is called a *Grassmann homomorphism* from $\mathcal{S}$ to $\mathcal{T}$ if $\varphi(S) \in \mathcal{T}$ holds for each $S \in \mathcal{S}$, and we will say that $\mathcal{S}$ is *Grassmann homomorphic* to $\mathcal{T}$, or briefly just that $\mathcal{S}$ is *homomorphic* to $\mathcal{T}$.

We adopt the arrow notation commonly used in graph theory; for any $\mathcal{S} \subseteq \mathrm{Gr}(V)$ and $\mathcal{T} \subseteq \mathrm{Gr}(W)$ we express the statement that $\mathcal{S}$ is homomorphic to $\mathcal{T}$ by writing $\mathcal{S} \to \mathcal{T}$. Without loss of generality we may assume $W = V$, if necessary by embedding the smaller of the two spaces into the larger. Thus $\to$ extends to a

relation on $\mathrm{Gr}(V)$, which clearly is reflexive and transitive, and, except for trivial cases, neither symmetric nor antisymmetric.

In the case of singleton $\mathcal{T} = \{T\}$ we write $\mathcal{S} \to T$ in place of $\mathcal{S} \to \mathcal{T}$. In particular $\mathcal{S} \to \mathbb{F}$ means that there exists $\varphi \in \mathcal{L}(V, \mathbb{F})$ such that $\varphi(S) = \mathbb{F}$ for each $S \in \mathcal{S}$.

Some elementary general observations follow readily from the definitions. They will be applied in the proofs of the theorems in Section 4 (Proposition 3 in the special case $d = 1$).

Let U, V and W be vector spaces.

Proposition 1. Let $\mathcal{R}, \mathcal{S}, \mathcal{T} \subseteq \mathrm{Gr}(V)$. If $\mathcal{R} \to \mathcal{S} \to \mathcal{T}$, then $\mathcal{R} \to \mathcal{T}$. In particular, if $\mathcal{R} \subseteq \mathcal{S}$, and $\mathcal{S} \to \mathcal{T}$, then $\mathcal{R} \to \mathcal{T}$. □

Proposition 2. If $\mathcal{S} \subseteq \mathrm{Gr}(U)$, $\mathcal{T} \subseteq \mathrm{Gr}^*(W)$, and $\mathcal{S} \to \mathcal{T}$, then $\mathcal{S} \subseteq \mathrm{Gr}^*(U)$. □

Proposition 3. Let $d \in \mathbb{N}$ and assume $\dim(U) = \dim(W) + d$. Then

(i) $\mathrm{Gr}(d, U) \not\to \mathrm{Gr}^*(W)$.
(ii) $\mathrm{Gr}(d, U) \setminus \{S\} \to \mathrm{Gr}^*(W)$ for each $S \in \mathrm{Gr}(d, U)$.

Proof. For (i), let $\varphi \in \mathcal{L}(U, W)$. Then

$$\dim(\ker \varphi) = \dim U - \dim(\mathrm{im}\ \varphi) \geq \dim U - \dim W = d.$$

It follows that $\ker \varphi$ has a subspace S with $S \in \mathrm{Gr}(d, U)$, implying $\varphi(S) \notin \mathrm{Gr}^*(W)$.

For (ii), assume $S \in \mathrm{Gr}(d, U)$. Then $\dim(U/S) = \dim U - d = \dim W$. There exists an isomorphism in $\mathcal{L}(U/S, W)$, which naturally induces a function $\varphi \in \mathcal{L}(U, W)$ with $\ker \varphi = S$, so $\varphi(\mathrm{Gr}(d, U) \setminus \{S\}) \subseteq \mathrm{Gr}^*(W)$. □

3. Examples and Complexity

We will encode some classical graph and hypergraph problems into the language of homomorphisms.

Example 1: Graph Coloring. Let $G = (V_G, E_G)$ be a nonempty finite graph, and let k be a natural number. A *k-coloring* of G is a function $c : V_G \to C$, where C is any set of size k, such that c satisfies the condition $c(u) \neq c(v)$ for each edge uv of G. The *chromatic number* $\chi(G)$ of G is the least value of k for which a k-coloring of G exists.

We assume in the following that $\mathbb{F}$ is finite and $k = |\mathbb{F}|$. To color G with a number of colors that is not a prime power, one may equivalently choose a prime power q larger than k, and instead consider to q-color the graph obtained from G by adding $q - k$ new pairwise adjacent vertices each of which is made adjacent to all vertices of G.

We may assume that V_G is a basis for V. For each edge $e = uv \in E_G$ let $\ell_e = \langle u - v \rangle$, and let $\mathcal{S} = \{\ell_e : e \in E_G\}$. Then the following equivalence holds.

$$\chi(G) \leq k \ \Leftrightarrow\ \mathcal{S} \to \mathbb{F}. \tag{1}$$

Indeed, assume the existence of a k-coloring $c : V_G \to \mathbb{F}$ of G. Let $\varphi : V \to \mathbb{F}$ be the function in $\mathcal{L}(V, \mathbb{F})$ given by $\varphi(v) = c(v)$ for each $v \in V_G$. Then for each $e = uv \in E_G$,

$$\varphi(u - v) = \varphi(u) - \varphi(v) = c(u) - c(v) \neq 0,$$

since $c(u) \neq c(v)$. Hence $\varphi(\ell_e) = \mathbb{F}$, for each $\ell_e \in \mathcal{S}$, and $\mathcal{S} \to \mathbb{F}$ follows. The converse is similar.

Example 2: Hypergraph Coloring. More generally, let $H = (V_H, E_H)$ be a nonempty finite hypergraph, that is, V_H is a finite set, and each element of the set of *hyperedges* E_H is a nonempty subset of V_H. For natural number k, a *k-coloring* of H is a function $c : V_H \to C$, where C is a set of size k, such that for every hyperedge $h \in E_H$ its image $c(h)$ contains at least two distinct colors, that is, h is not *monochromatic*. The *chromatic number* $\chi(H)$ of H is the least number k for which such a k-coloring exists, if one exists. If H has a singleton hyperedge, then no coloring exists, and we write $\chi(H) = \infty$.

If k is not a prime power, as before we may, for some prime power $q > k$, add $q-k$ new vertices, and for each such new vertex v add all possible 2-element hyperedges that contain v as an element, and equivalently consider q-colorings of the larger hypergraph instead.

As before, we assume that V_H is a basis for V. For each hyperedge $h \in E_H$ let S_h be the subspace of V defined by

$$S_h = \left\{ \sum_{v \in h} \alpha_v v \ : \ \sum_{v \in h} \alpha_v = 0 \right\}.$$

Let $\mathcal{S} = \{S_h : h \in E_H\}$. Then

$$\chi(H) \leq k \ \Leftrightarrow \ \mathcal{S} \to \mathbb{F}. \tag{2}$$

To see the forward implication, assume $k = |\mathbb{F}|$, and that a k-coloring $c : V_H \to \mathbb{F}$ of H exists. Then extend c to the function $\varphi \in \mathcal{L}(V, \mathbb{F})$ for which $\varphi(v) = c(v)$ for every $v \in V_H$. For each $h \in E_H$ we then have

$$\varphi(S_h) = \left\{ \sum_{v \in h} \alpha_v c(v) \ : \ \sum_{v \in h} \alpha_v = 0 \right\}.$$

By assumption, there exist elements $u, v \in h$ with $c(u) \neq c(v)$. With $\alpha_u = 1$, $\alpha_v = -1$, and $\alpha_w = 0$ for all $w \in h \setminus \{u, v\}$, this implies $0 \neq u - v \in \varphi(S_h)$, implying $\varphi(S_h) = \mathbb{F}$, and hence $\mathcal{S} \to \mathbb{F}$.

Conversely, assume $\mathcal{S} \to \mathbb{F}$. Then there exists $\varphi \in \mathcal{L}(V, \mathbb{F})$ for which $\varphi(S_h) = \mathbb{F}$ for every hyperedge $h \in E_H$. Using the definition of S_h, this implies that φ is not constant on any $h \in E_H$, and it follows that φ defines a k-coloring of H.

Example 3: Nowhere-Zero Flow. An *orientation* $\vec{G}$ of G is an assignment to each edge $e = uv$ of G of a *head* $h(e)$ and a *tail* $t(e)$, that is, $\vec{G}(e) = (h(e), t(e))$, where $\{h(e), t(e)\} = \{u, v\}$. A *nowhere-zero k-flow* in G is a pair $(\vec{G}, \psi)$, where $\vec{G}$ is an orientation of G and $\psi : E_G \to \{-k+1, \ldots, -1, 1, \ldots, k-1\}$ satisfies *Kirchhoff's Law* of flow conservation:

$$\sum_{\{e \in E \,:\, h(e) = v\}} \psi(e) - \sum_{\{e \in E \,:\, t(e) = v\}} \psi(e) = 0 \quad \text{for all } v \in V_G.$$

If $\mathcal{A}$ is any additive Abelian group, a *nowhere-zero $\mathcal{A}$-flow* in G is defined similarly, that is, ψ is a function from E_G to $\mathcal{A} \setminus \{0_{\mathcal{A}}\}$, satisfying flow conservation at every vertex, where $0_{\mathcal{A}}$ is the zero-element of $\mathcal{A}$. Tutte [18] proved that there exists a nowhere-zero k-flow in G if and only if there exists a nowhere-zero $\mathcal{A}$-flow in G for every Abelian group $\mathcal{A}$ with precisely k elements. Tutte also proved that 'every Abelian group' can be replaced by 'any Abelian group'.

Assume that E_G is a basis for the vector space W. Fix any orientation $\vec{G}$ of G. We define a function $\sigma : V_G \times E_G \to \mathbb{F}$ by

$$\sigma(v,e) = \begin{cases} 1 & \text{if } v = h(e) \\ -1 & \text{if } v = t(e) \\ 0 & \text{otherwise} \end{cases}$$

Let F be the set of all functions $f \in \mathcal{L}(W, \mathbb{F})$ that satisfy the Kirchhoff condition

$$\sum_{e \in E_G} \sigma(v,e) f(\ell_e) = 0 \quad \text{for all } v \in V_G$$

It is easy to check that F is a vector space over $\mathbb{F}$ of finite dimension.

For each $e \in E_G$ let the function g_e be defined by $g_e(f) = f(\ell_e)$ for all $f \in F$. Then $g_e \in \mathcal{L}(F, \mathbb{F})$ for all $e \in E_G$. Let $\mathcal{Q}$ be the set of all lines in $\mathcal{L}(F, \mathbb{F})$ of the form $\{\alpha g_e : \alpha \in \mathbb{F}\}$ with $e \in E_G$. Then $\mathcal{Q}$ is a set of subspaces of the finite dimensional vector space $\mathcal{L}(F, \mathbb{F})$, and

$$G \text{ admits a nowhere-zero } k\text{-flow} \;\Leftrightarrow\; \mathcal{Q} \to \mathbb{F}. \tag{3}$$

To see the forward implication, assume the existence of a nowhere-zero k-flow for G. Applying the theorem of Tutte to the Abelian additive group of $\mathbb{F}$, there is a function $\psi : E_G \to \mathbb{F}$ which together with $\vec{G}$ defines a nowhere-zero $\mathbb{F}$-flow in G. Let d be the dimension of the vector space F over $\mathbb{F}$, and choose a basis $f_1, f_2, \ldots, f_d$ for F. Let $a_1, a_2, \ldots, a_d \in \mathbb{F}$ be the coefficients for which $\sum_{i=1}^{d} a_i f_i = \psi$. For each $g \in \mathcal{L}(F, \mathbb{F})$ let

$$\Phi(g) = \sum_{i=1}^{d} a_i g(f_i).$$

Then Φ is a linear function from $\mathcal{L}(F, \mathbb{F})$ to $\mathbb{F}$, and for each $e \in E_G$,

$$\Phi(g_e) = \sum_{i=1}^{d} a_i g_e(f_i) = \sum_{i=1}^{d} a_i f_i(e) = \psi(e) \neq 0,$$

thus implying $\mathcal{Q} \to \mathbb{F}$.

Conversely, assume that $\Phi : \mathcal{L}(F, \mathbb{F}) \to \mathbb{F}$ is linear, with $\Phi(\mathcal{Q}) = \{\mathbb{F}\}$. For each edge $e \in E_G$ let $\psi(e) = \Phi(g_e)$. Then $\psi(e) \neq 0$, and for each $v \in V$ we have

$$\sum_{e \in E_G} \sigma(v,e)\psi(e) = \sum_{e \in E_G} \sigma(v,e)\Phi(g_e) = \Phi\Big(\sum_{e \in E_G} \sigma(v,e) g_e\Big),$$

and for every $f \in F$,

$$\left(\sum_{e \in E_G} \sigma(v,e) g_e\right)(f) = \sum_{e \in E_G} \sigma(v,e) g_e(f) = \sum_{e \in E_G} \sigma(v,e) f(\ell_e) = 0.$$

Hence $\sum_{e \in E_G} \sigma(v,e)\psi(e) = \Phi(0) = 0$, so $(\vec{G}, \psi)$ is a nowhere-zero $\mathbb{F}$-flow in G. By Tutte's theorem, there exists a nowhere-zero k-flow in G.

Example 4: Zero-Sum Flow. The undirected analogue of a nowhere-zero $\mathcal{A}$-flow in a graph G, for an Abelian group $\mathcal{A}$, is called a *zero-sum $\mathcal{A}$-flow*, and it is a function $\psi : E_G \to \mathcal{A} \setminus \{0_{\mathcal{A}}\}$ with the property

$$\sum_{uv \in E_G} \psi(uv) = 0 \quad \text{for all } v \in V_G,$$

that is, the sum of the values of ψ on the edges incident to any vertex v of G is zero.

Let Z be the set of functions $\psi : E_G \to \mathbb{F}$ for which

$$\sum_{\{u \in V_G \,:\, uv \in E_G\}} \psi(uv) = 0 \quad \text{for all } v \in V_G.$$

For each $e \in E_G$ define $z_e : Z \to \mathbb{F}$ by $z_e(\psi) = \psi(e)$, and let $\mathcal{R} = \{\langle z_e \rangle : e \in E_G\}$. Then

$$G \text{ admits a zero-sum } \mathbb{F}\text{-flow} \;\Leftrightarrow\; \mathcal{R} \to \mathbb{F}. \tag{4}$$

The argument is similar to that of Example 3.

Proposition 4. For fixed positive integer d and fixed prime power k, the problem of deciding $\mathcal{S} \to \mathbb{F}$ for input $n \in \mathbb{N}$ and $\mathcal{S} \subseteq \mathrm{Gr}(d, \mathbb{F}^n)$ is polynomially decidable for $|\mathbb{F}| = k$ if $(d, k) = (1, 2)$, and otherwise it is NP-complete.

Proof. It was proved by Karp [8] that for fixed $k > 2$ it is NP-complete to decide whether a graph is k-colorable. By Example 1, this problem is equivalent to deciding $\mathcal{S} \to \mathbb{F}$ for an input $\mathcal{S} \subseteq \mathrm{Gr}(1, \mathbb{F}^n)$, where n is the order of the input graph. Since the latter problem is in NP, it follows that it is NP-complete.

For $k \geq 2$ and fixed $m \geq 3$ it is NP-complete to decide whether an m-uniform hypergraph (i.e. all hyperedges have size m) is k-colorable. This follows from a theorem by Lovász [12]. Since by Example 2 this reduces to deciding $\mathcal{S} \to \mathbb{F}$ for input $\mathcal{S} \subseteq \mathrm{Gr}(d, \mathbb{F}^n)$, where $d = m - 1$ and n is the order of the hypergraph, this problem is also NP-complete.

For $k = 2$ and $d = 1$ the problem becomes deciding $\mathcal{S} \to \mathbb{F}$ for input $\mathcal{S} \subseteq \mathrm{Gr}(1, \mathbb{F}^n)$, when $|\mathbb{F}| = 2$. Assume that $\mathcal{S}$ contains the lines $\langle v_1 \rangle, \langle v_2 \rangle, \ldots, \langle v_r \rangle$, where $v_1, v_2, \ldots, v_r \in \mathbb{F}^n \setminus \{0\}$. Let $X \subseteq \mathbb{F}^n$ be the subspace $X = \langle v_1, v_2, \ldots, v_r \rangle$. It is easy to calculate a basis $B \subseteq \{v_1, v_2, \ldots, v_r\}$ for X. Then each v_i is a sum of the elements of an easily calculated subset $A_i \subseteq B$, for $1 \leq i \leq r$. Any function $\varphi \in \mathcal{L}(\mathbb{F}^n, \mathbb{F})$ that satisfies $\varphi(\langle v_i \rangle) = \mathbb{F}$ satisfies $\varphi(v_i) = 1$, so by linearity of φ, and since the characteristic of $\mathbb{F}$ is 2, $\mathcal{S} \to \mathbb{F}$ holds if and only if A_i contains an odd number of elements for each $i = 1, 2, \ldots, r$, which is easily checked in polynomial time. □

4. Hajós-type Theorems

This section describes three different constructions of those sets $\mathcal{S} \subseteq \mathrm{Gr}(1, V)$ for which $\mathcal{S} \not\to \mathbb{F}$ holds. The operations (i) and (ii) introduced by Hajós [3] are special cases of the operations used in the third, and in a sense weakest, of these, while the operations (i) and (ii)' studied by Pitassi and Urquhart [17] are special cases of the operations used in the second of the constructions. The first of the three constructions is more restrictive than the other two and it has no counterpart for graphs. The constructions in Theorem 2 and Theorem 3 are less restrictive, and the proof of each is based on Theorem 1.

Assume $\mathcal{P}, \mathcal{Q} \subseteq \mathrm{Gr}(1, V)$ satisfy $\mathcal{P} \setminus \mathcal{Q} = \{\ell_1\}$ and $\mathcal{Q} \setminus \mathcal{P} = \{\ell_2\}$, and there exist $x_1, x_2 \in V$ such that $\ell_1 = \langle x_1 \rangle$ and $\ell_2 = \langle x_2 \rangle$, and the line $\ell = \langle x_1 + x_2 \rangle$ is an element of $\mathcal{P} \cap \mathcal{Q}$. Then we say that $\mathcal{R} = \mathcal{P} \cap \mathcal{Q}$ is obtained from $(\mathcal{P}, \mathcal{Q})$ by *elimination*.

Proposition 5. If $\mathcal{R}$ is obtained from $(\mathcal{P}, \mathcal{Q})$ by elimination, then

$$\mathcal{R} \to \mathbb{F} \;\Rightarrow\; \mathcal{P} \to \mathbb{F} \vee \mathcal{Q} \to \mathbb{F}.$$

Proof. Assume that $H : V \to \mathbb{F}$ is linear and satisfies $H(\mathcal{R}) = \{\mathbb{F}\}$. We assume $\mathcal{R} = \mathcal{P} \setminus \{\ell_1\} = \mathcal{Q} \setminus \{\ell_2\}$, and $\ell = \langle x_1 + x_2 \rangle \in \mathcal{R}$ for some $x_i \in \ell_i$, for $i = 1, 2$. Then $\ell \in \mathcal{R}$ and $H(\mathcal{R}) = \{\mathbb{F}\}$ implies $H(\ell) = \mathbb{F}$ hence $H(x_1 + x_2) \neq 0$. So one of $H(x_1) \neq 0$ and $H(x_2) \neq 0$ holds, implying $H(\ell_1) = \mathbb{F}$ or $H(\ell_2) = \mathbb{F}$.

It follows that at least one of $H(\mathcal{P}) = H(\mathcal{R} \cup \{\ell_1\}) = \{\mathbb{F}\}$ and $H(\mathcal{Q}) = H(\mathcal{R} \cup \{\ell_2\}) = \{\mathbb{F}\}$ is satisfied. □

For a subspace S of V we refer to the set $\mathcal{V}_S = \{\ell \in \mathrm{Gr}(1, V) : \ell \not\subseteq S\}$ of lines not contained in S as the *co-pencil* of S in V. A co-pencil $\mathcal{V}_S$ of S is *strong* if $\dim V \geq 2 + \dim S$.

Proposition 6. If $\mathcal{V}_S$ is a strong co-pencil, and U is any 2-dimensional vector space, then $\mathrm{Gr}(1, U) \to \mathcal{V}_S$.

Proof. It follows from $\dim V \geq 2 + \dim S$ that there exists a 2-dimensional subspace W of V for which $S \cap W$ is trivial. Then $\mathrm{Gr}(1, U) \to \mathcal{V}_S$ follows by choosing any isomorphism from U to W. □

Proposition 7. If S is a subspace of V, then

$$\mathcal{V}_S \not\to \mathbb{F} \;\Leftrightarrow\; \mathcal{V}_S \text{ is strong.}$$

Proof. We first show ($\Rightarrow$). Assume $\dim V \leq 1 + \dim S$. If $S = V$, then $\mathcal{V}_S = \emptyset$, and $\mathcal{V}_S \to \mathbb{F}$ is trivially true. So we may assume $V = \{v + \lambda x : v \in S, \lambda \in \mathbb{F}\}$ for some $x \in \ell \in \mathcal{V}_S$. Now $v + \lambda x \mapsto \lambda$ defines a linear function from V to $\mathbb{F}$ which maps every element of $\mathcal{V}_S$ to $\mathbb{F}$. This shows $\mathcal{V}_S \to \mathbb{F}$.

Conversely, assume that $\mathcal{V}_S$ is strong. Let U be any 2-dimensional vector space. Part (i) of Proposition 3 (with $d = 1$, and $W = \mathbb{F}$) implies $\mathrm{Gr}(1, U) \not\to \mathbb{F}$. Hence $\mathcal{V}_S \not\to \mathbb{F}$ follows by Propositions 1 and 6. □

Next we state and prove the first general construction of sets of lines that are not homomorphic to $\mathbb{F}$. The subsequent constructions in Theorem 2 and Theorem 3 are deduced from Theorem 1.

Theorem 1. *Let $\mathbb{F}$ be a finite field and let V be a vector space over $\mathbb{F}$ of finite dimension. Let $\mathcal{P} \subseteq \mathrm{Gr}(1, V)$. Then $\mathcal{P} \not\to \mathbb{F}$ if and only if there exist a natural number $N \geq 1$ and a sequence $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_N$ for which $\mathcal{R}_N = \mathcal{P}$, such that for all $i = 1, 2, \ldots, N$,*

(i) *$\mathcal{R}_i$ is a strong co-pencil, or*
(ii) *$\mathcal{R}_i$ is obtained from $(\mathcal{R}_{j_1}, \mathcal{R}_{j_2})$ by elimination, for some j_1, j_2 with $1 \leq j_1, j_2 < i$.*

Proof. The "if" direction follows by induction on N from Propositions 5 and 7.

So we assume $\mathcal{P} \not\to \mathbb{F}$. Let F be the set of all elements v of V for which $\langle v \rangle \notin \mathcal{P}$. Clearly $0 \in F$, so F is nonempty, and if $v \in F$, then $\langle v \rangle \subseteq F$. The proof of "only if" proceeds by induction on $n = |F| \geq 1$.

If F is a subspace of V, then $\mathcal{P} = \mathcal{V}_F$, and we let $N = 1$ and $\mathcal{R}_1 = \mathcal{P}$. Then $\mathcal{R}_1$ is the co-pencil of F, and by Proposition 7, $\mathcal{R}_1$ is strong. Hence the statement of the theorem is satisfied.

We may now assume that F is not a vector space. We choose $f_1, f_2 \in F$ so that $f_1 + f_2 \notin F$.

By the induction hypothesis applied to $\mathcal{P} \cup \{\langle f_1 \rangle\}$, there exist a natural number N_1 and a sequence $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_{N_1}$, with $\mathcal{R}_{N_1} = \mathcal{P} \cup \{\langle f_1 \rangle\}$, such that (i) and (ii) hold for all $i = 1, 2, \ldots, N_1$.

Similarly, by applying the hypothesis to $\mathcal{P} \cup \{\langle f_2 \rangle\}$, there exist a natural number N_2 and a sequence $\mathcal{R}_{N_1+1}, \mathcal{R}_{N_1+2}, \ldots, \mathcal{R}_{N_1+N_2}$, with $\mathcal{R}_{N_1+N_2} = \mathcal{P} \cup \{\langle f_2 \rangle\}$, such that (i) and (ii) hold for $i = N_1 + 1, N_1 + 2, \ldots, N_1 + N_2$.

Since $f_1 + f_2 \notin F$ implies $\langle f_1 + f_2 \rangle \in \mathcal{P}$, we finally obtain $\mathcal{P}$ from $(\mathcal{P} \cup \{\langle f_1 \rangle\}, \mathcal{P} \cup \{\langle f_2 \rangle\})$ by elimination. Hence with $N = N_1 + N_2 + 1$ and $\mathcal{R}_N = \mathcal{P}$, the sequence $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_N$ satisfies the statement of the theorem. □

Theorem 2. *Let $\mathbb{F}$ be a finite field and let V be a vector space over $\mathbb{F}$ of finite dimension. Let $\mathcal{P} \subseteq \mathrm{Gr}(1, V)$. Then $\mathcal{P} \not\to \mathbb{F}$ if and only if there is a natural number $N \geq 0$ and a sequence $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_N$, for which $\mathcal{R}_0 = \mathrm{Gr}(1, \mathbb{F}^2)$ and $\mathcal{R}_N = \mathcal{P}$, such that for all $i = 1, 2, \ldots, N$,*

(i) *$\mathcal{R}_j \to \mathcal{R}_i$ for some j with $0 \leq j < i$, or*
(ii) *R_i is obtained from $(\mathcal{R}_{j_1}, \mathcal{R}_{j_2})$ by elimination, for some j_1, j_2 with $1 \leq j_1, j_2 < i$.*

Proof. The "if" direction follows from Propositions 1–3 and 5.

To show "only if", let $\mathcal{R}_1, \ldots, \mathcal{R}_N$ be any sequence as in Theorem 1, and let $\mathcal{R}_0 = \mathrm{Gr}(1, \mathbb{F}^2)$. It follows from Theorem 1 and Proposition 6 that $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_N$ satisfy (i) and (ii). □

Definition 2. Let $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathrm{Gr}(1, V)$ be two sets of lines in V. A set of lines $\mathcal{S} \subseteq \mathrm{Gr}(1, V)$ is a 2-*sum* of $\mathcal{S}_1$ and $\mathcal{S}_2$ if there exist V_i, ℓ_i, x_i for $i = 1, 2$ for which

- V_1, V_2 are subspaces of V such that $V = V_1 \oplus V_2$,
- $\mathcal{S}_i \subseteq \mathrm{Gr}(1, V_i)$, for $i = 1, 2$,
- $\ell_i \in \mathcal{S}_i$, for $i = 1, 2$,
- $\ell_i = \langle x_i \rangle$, for $i = 1, 2$,
- $\mathcal{S} = (\mathcal{S}_1 \cup \mathcal{S}_2 \cup \{\ell\}) \setminus \{\ell_1, \ell_2\}$, where $\ell = \langle x_1 + x_2 \rangle$.

Proposition 8. If $\mathcal{S}$ is a 2-sum of $\mathcal{S}_1$ and $\mathcal{S}_2$, where $\mathcal{S}_i \not\to \mathbb{F}$, for $i = 1, 2$, then $\mathcal{S} \not\to \mathbb{F}$.

Proof. Let $V_1, V_2, \mathcal{S}_1, \mathcal{S}_2, \ell_1, \ell_2, \ell$ be as in the definition of a 2-sum. Let $\varphi \in \mathcal{L}(V, \mathbb{F})$, and suppose $\varphi(\mathcal{S}) = \mathbb{F}$. Then $\mathcal{S}_i \setminus \{\ell_i\} \subseteq \mathcal{S}$ and $\mathcal{S}_i \not\to \mathbb{F}$ imply $\varphi(\ell_i) = 0$, which again implies $\varphi(x_i) = 0$, for $i = 1, 2$. Then $\varphi(x_1 + x_2) = 0$ follows by linearity, which implies $\varphi(\ell) = 0$, contradicting $\varphi(\mathcal{S}) = \{\mathbb{F}\}$. □

Proposition 9. If $\mathcal{R}$ is obtained from $(\mathcal{P}, \mathcal{Q})$ by elimination, then there exists a sequence $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_6$ with $\mathcal{S}_1 = \mathcal{P}$, $\mathcal{S}_2 = \mathcal{Q}$, and $\mathcal{S}_6 = \mathcal{R}$, such that for $i = 3, 4, 5, 6$,

(i) $\mathcal{S}_j \to \mathcal{S}_i$ for some j with $1 \leq j < i$, or
(ii) $\mathcal{S}_i$ is a 2-sum of S_{j_1} and S_{j_2} for some j_1, j_2 with $1 \leq j_1, j_2 < i$.

Proof. Assume $x_1, x_2 \in V$, $\ell_1 = \langle x_1 \rangle$, $\ell_2 = \langle x_2 \rangle$, $\mathcal{P} \setminus \mathcal{Q} = \{\ell_1\}$, $\mathcal{Q} \setminus \mathcal{P} = \{\ell_2\}$, $\mathcal{R} = \mathcal{P} \cap \mathcal{Q}$, and $\ell = \langle x_1 + x_2 \rangle \in \mathcal{R}$, so that $\mathcal{R}$ is obtained by elimination from $(\mathcal{P}, \mathcal{Q})$.

Let V_1' and V_2' be two vector spaces each of which is isomorphic to V, chosen so that $V_1' \cap V_2' = \{0\}$, and let $V' = V_1' \oplus V_2'$. For $i = 1, 2$ choose $\varphi_i \in \mathcal{L}(V, V')$ for which $\varphi_i(V) = V_i'$, and let $\mathcal{S}_i' = \varphi_i(\mathcal{S}_i)$, $\ell_i' = \varphi_i(\ell_i)$, and $x_i' = \varphi_i(x_i)$. In particular $\mathcal{S}_i \to \mathcal{S}_i'$ holds for $i = 1, 2$. Let $\ell' = \langle x_1' + x_2' \rangle$ and $\mathcal{R}' = \mathcal{S}_1' \cup \mathcal{S}_2' \cup \{\ell'\}) \setminus \{\ell_1', \ell_2'\}$; then $\mathcal{R}'$ is a 2-sum of $\mathcal{S}_1'$ and $\mathcal{S}_2'$.

Define $\varphi : V' \to V$ by $\varphi(y_1 + y_2) = \varphi_1^{-1}(y_1) + \varphi_2^{-1}(y_2)$ whenever $y_i \in V_i'$ for $i = 1, 2$. Then φ is linear, and $\varphi(\mathcal{R}') = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \{\varphi(\ell')\} \setminus \{\ell_1, \ell_2\}$. Since $\mathcal{S}_1 = \mathcal{P}$, $\mathcal{S}_2 = \mathcal{Q}$, and

$$\varphi(\ell') = \varphi(\langle x_1' + x_2' \rangle) = \langle \varphi(x_1' + x_2') \rangle = \langle \varphi(x_1') + \varphi(x_2') \rangle = \langle x_1 + x_2 \rangle = \ell,$$

it follows that $\varphi(\mathcal{R}') = \mathcal{R}$, hence $\mathcal{R}' \to \mathcal{R}$.

Now the sequence

$$\mathcal{S}_1 = \mathcal{P}, \mathcal{S}_2 = Q, \mathcal{S}_3 = \mathcal{S}_1', \mathcal{S}_4 = \mathcal{S}_2', \mathcal{S}_5 = \mathcal{R}', \mathcal{S}_6 = \mathcal{R}$$

satisfies the statement of the Proposition. □

Theorem 3. *Let $\mathbb{F}$ be a finite field and let V be a vector space over $\mathbb{F}$ of finite dimension. Let $\mathcal{P} \subseteq \mathrm{Gr}(1, V)$. Then $\mathcal{P} \not\to \mathbb{F}$ if and only if there is a natural number $N \geq 0$ and a sequence $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_N$, for which $\mathcal{R}_0 = \mathrm{Gr}(1, \mathbb{F}^2)$ and $\mathcal{R}_N = \mathcal{P}$, such that for all $i = 1, 2, \ldots, N$,*

(i) *$\mathcal{R}_j \to \mathcal{R}_i$ for some j with $0 \leq j < i$, or*
(ii) *$\mathcal{R}_i$ is a 2-sum of $\mathcal{R}_{j_1}$ and $\mathcal{R}_{j_2}$ for some j_1, j_2 with $0 \leq j_1, j_2 < i$.*

Proof. The "if" direction follows from Propositions 1–3 and 8.

The converse follows from Theorem 2 and Proposition 9. □

The final theorem is more closely related than the two previous theorems to the original Hajós Theorem [3] on the construction of graphs with a given lower bound on chromatic number. The operation (i) corresponds to usual homomorphism of graphs; this may be viewed as repeated application of vertex identification, which is the operation that features in the Hajós Theorem. Operation (ii) is a generalization of the *Hajós operation* of combining two graphs to produce a larger graph.

Theorem 3 is also similarly related to the generalization proved by Jaeger [6] of the Hajós Theorem to constructions of matroids representable over finite fields and satisfying a property of having a large 'critical exponent' that essentially generalizes the graph property of chromatic number exceeding k, and dually the property of a graph not to allow a nowhere-zero k-flow for a prime power value of k. The formulation of Jaeger's Theorem and its proof becomes tedious in the matroid formulation, since there is no apparent natural concept of 'homomorphism' for abstract matroids, though one can be manufactured in the special case of representable matroids. There is a natural matroid associated with a subset S of $\mathrm{Gr}(1, \mathbb{F})$, that has as its elements one nonzero point on each line in S, so that matroid independence is given by linear independence. The statement $S \to \mathbb{F}$ allows restating as a statement about the critical exponent for this matroid. Theorem 3 then allows a restatement in the language of Jaeger's Theorem; however, the proof given by Jaeger [6] is quite different from the present.

References

[1] G.A. Dirac, A theorem of R.L. Brooks and a conjecture of H. Hadwiger, *Proc. London Math. Soc. (3)* **7** (1957), 161–195.
[2] S. Gravier, A Hajós-like theorem for list coloring, *Discrete Math.* **152** (1996), 299–302.
[3] G. Hajos, Über eine Konstruktion nicht n-färbbärer Graphen, *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg* **A10** (1961), 116–117.
[4] D. Hanson, G.C. Robinson and B. Toft, Remarks on the graph colour theorem of Hajós, in: *Proc. 17th S-E Conference on Combinatorics, Graph Theory and Computing, Boca Raton, 1986, Congr. Num.* **55**, pp. 69–76, 1986.

[5] K. Iwama, K. Seto and S. Tamaki, The complexity of the Hajós calculus for planar graphs *Theoret. Comput. Sci.* **411** (2010), 1182–1191
[6] F. Jaeger, A constructive approach to the critical problem for matroids, *Europ. J. Combin.* **2** (1981), 137–144.
[7] T.R. Jensen and G.F. Royle, Hajós constructions of critical graphs, *J. Graph Theory* **30** (1999), 37–50.
[8] R.M. Karp, Reducibility among combinatorial problems, in R.E. Miller and J.W. Thatcher, eds., *Complexity of Computer Computations*, Plenum Press, New York 1972, pp. 85–103.
[9] G. Koester, On 4-critical planar graphs with high edge density, *Discrete Math.* **98** (1991), 147–151.
[10] D. Král, Hajós' theorem for list coloring, *Discrete Math.* **287** (2004), 161–163.
[11] S. Liu and J. Zhang, Using Hajós construction to generate hard graph 3-colorability instances, Artificial Intelligence and Symbolic Computation, Lecture Notes in Computer Science 4120, Springer-Verlag 2006, pp. 211–225.
[12] L. Lovász, Coverings and colorings of hypergraphs, in *Proc. 4th S.-E. Conference on Combinatorics, Graph Theory and Computing*. Utilitas Mathematica Publishing, Winnipeg 1973, pp. 3–12.
[13] A.J. Mansfield and D.J.A. Welsh, Some colouring problems and their complexity, *Graph theory (Cambridge, 1981)*, North-Holland Math. Stud. 62, Amsterdam, North-Holland 1982, pp. 159–170.
[14] J. Nešetřil, The Homomorphism Structure of Classes of Graphs, *Combin. Probab. Comput.* **8** (1999), 177–184.
[15] O. Ore, *The Four-Color Problem*, Academic Press 1967.
[16] J.G. Oxley, *Matroid Theory*, Oxford University Press 2006.
[17] T. Pitassi and A. Urquhart, The complexity of the Hajós calculus, *SIAM J. Disc. Math.* **8** (1995), 464–483.
[18] W.T. Tutte, A contribution to the theory of chromatic polynomials, *Canad. J. Math.* **6** (1954), 80–91
[19] W.T. Tutte, On the algebraic theory of graph colorings, *J. Combin. Theory* **1** (1966), 15–50.
[20] W.T. Tutte, A lecture on graph-colourings, C&O Department, University of Waterloo, Canada, June 26, 1992.
[21] X. Zhu, An analogue of Hajós' theorem for circular chromatic number, *Proc. Amer. Math. Soc.* **129** (2001), 2845–2852.
[22] X. Zhu, An analogue of Hajós' theorem for circular chromatic number (II), *Graphs Comb.* **265** (2003), 419–432.

Tommy Rene Jensen
Kyungpook National University,
1370-1 Sangyeok, Buk-gu
702-701 Daegu, Republic of Korea
E-mail address: tjensen@knu.ac.kr