VECTOR REPRESENTABLE MATROIDS OF GIVEN RANK WITH GIVEN AUTOMORPHISM GROUP

László BABAI
Dept. Algebra and Number Theory, Eötvös L. University, H-1088 Budapest, Hungary

Received 25 August 1977
Revised 29 May 1978

A simple way of associating a matroid of prescribed rank with a graph is shown. The matroids so constructed are representable over any sufficiently large field. Their use is demonstrated by the following result: Given an integer \( k \geq 3 \) and a function \( G \) associating a group with each subset of a set \( S \), there is a matroid \( M(E) \), representable over any sufficiently large field, such that \( E = S \), and for any \( T \subseteq S \), the rank of \( M \setminus T \) is \( k \), and the automorphism group of \( M \setminus T \) is isomorphic to \( G(T) \).

1. Introduction

By matroids we mean both finite and infinite ones, but of finite rank only. For matroid terminology we refer to [11, 1].

Automorphisms of a matroid \( M = M(E) \) are isomorphisms of \( M \) onto itself. \( \text{Aut } M \) denotes the group of automorphisms of \( M \); whence it consists of those permutations of the set \( E \) which preserve both independence and dependence. (The latter is not a consequence of the former one if \( E \) is infinite.) For a graph \( X \) without parallel edges, the automorphism group \( \text{Aut } X \) is defined similarly, as a permutation group acting on the set of vertices. It is well known (Frucht [3]) that any finite group is isomorphic to \( \text{Aut } X \) for some finite graph \( X \). This graph may be required to be 3-connected. As the isomorphisms of the circuit matroids of 3-connected graphs are just the mappings induced by graph isomorphisms (Whitney [12]), it follows that any finite group is isomorphic to \( \text{Aut } M \) for some graphic matroid \( M \). The ranks of these matroids are, however, unbounded. This is necessarily so for matroids, representable over a fixed finite field (not only for graphic ones).

Mendelsohn [9] has proved that any (finite or infinite) group is isomorphic to the automorphism group of some projective plane. A projective plane being a rank 3 matroid, we obtain a positive answer to the question whether the rank of \( M \) with \( \text{Aut } M \cong G \) may be bounded. It is, however, a disadvantage of this construction that it associates infinite planes with finite groups, and, of course, the resulting planes are not vector-representable.

The aim of the present note is to solve both problems. We shall exhibit matroids of prescribed rank and automorphism group, representable over any
sufficiently large field (Theorem 3.1). Using a result of the author on automorphism groups of graphs, we derive that the automorphism group of several restrictions of a vector representable matroid of rank $k$ (obtained by deleting subsets of a fixed subset of the underlying set) can be prescribed independently (Theorem 3.2, see the abstract).

The proof of these results is based on the following simple construction.

**Definition 1.1.** Let $k \geq 3$ be a positive integer and let $X = (V, E)$ be a (finite or infinite) graph. (Loops and parallel edges are admitted.) The rank-$k$ star matroid of $X$, denoted by $S_k(X)$ is defined as follows:

$$S_k(X) = M(E);$$

$H \subseteq E$ is independent in $M$ if either $|H| < k-1$, or $|H| = k$ and there is no vertex incident to all edges in $H$.

**Remark 1.2.** It is clear by definition that the rank of $S_k(X)$ never exceeds $k$, and $rk(S_k(X)) = k$ if and only if $X$ has at least $k$ edges and no point common to all edges of $X$.

We shall prove that the matroids $S_k(X)$ are representable over any sufficiently large field (Theorem 2.5 and Remark 2.6). Ideas due to Atkin [1] are employed to obtain an effective bound for this minimum size. On the other hand, if each vertex of $X$ has degree $\geq k$, $k \geq 3$, then the automorphism groups of $X$ and $S_k(X)$ are isomorphic (Lemma 2.1). This simple observation enables us to apply known results on automorphism groups of graphs to matroids.

2. Preliminaries

**Lemma 2.1.** Let $X = (V, E)$ be a (finite or infinite) graph without loops and parallel edges. Let $k \geq 3$ and assume that each vertex of $G$ has degree $\geq k$. Then

$$\text{Aut } X \cong \text{Aut } S_k(X).$$

**Proof.** Let $A_1(X)$ denote the group of permutations of $E$ induced by $\text{Aut } X$. By our assumption, obviously, $A_1(X) \cong \text{Aut } X$.

We assert that $A_1(X) = \text{Aut } M$ where $M = M(E) = S_k(X)$. Clearly, $A_1(X) \subseteq \text{Aut } M$.

For $v \in V$, let $E_v$ denote the star of $v$, i.e., the set of edges, incident with $v$. Let us observe, that the sets $H = E_v$ ($v \in V$) have the following properties:

(a) $|H| \geq k$;
(b) $rk(H) = k - 1$ (in $M$);
(c) $H$ is maximal with respect to (a) and (b).

Since clearly no subsets of $E$ other than the $E_v$'s have these properties, it
follows, that any automorphism $\alpha \in \text{Aut} M$ permutes the $E_v$'s: given $\alpha \in \text{Aut} M$ there is a permutation $\beta$ of $V$ such that
\[
\alpha E_v = E_{\beta v} \quad (v \in V).
\]
For $v, w \in V$, $v \neq w$ we have $|E_v \cap E_w| = 1$ or 0 depending on whether $v$ and $w$ are adjacent or not. The cardinality of $E_v \cap E_w$ being preserved by $\alpha$, it follows that $\beta \in \text{Aut} X$. For $e = \{v, w\} \in E$ we have $\{e\} = E_v \cap E_w$, $\{ae\} = E_{\beta v} \cap E_{\beta w}$, hence $\alpha$ is induced by $\beta, \alpha \in A_1(X)$. \hfill $\Box$

**Lemma 2.2.** Let $x_1, \ldots, x_6$ be distinct variables and $F$ a field.

Let $\beta_i, \gamma_i$ ($i = 1, 2, 3$) denote not necessarily different positive integers $\leq 6$. The determinant
\[
\begin{vmatrix}
1 & 1 & 1 \\
x_{\beta_i} + x_{\gamma_i} & x_{\beta_i} + x_{\gamma_i} & x_{\beta_i} + x_{\gamma_i} \\
x_{\beta_i} x_{\gamma_i} & x_{\beta_i} x_{\gamma_i} & x_{\beta_i} x_{\gamma_i}
\end{vmatrix}
\]
vanishes (as a polynomial in $F[x_1, \ldots, x_6]$) if and only if either

(a) $\{\beta_i, \gamma_i\} = \{\beta_j, \gamma_j\}$ for some $1 \leq i < j \leq 3$; or

(b) $\bigcap_{i=1}^3 \{\beta_i, \gamma_i\} \neq \emptyset$; or

(c) $\beta_i = \gamma_i (i = 1, 2, 3)$ and $F$ has characteristic 2.

**Proof.** Let $t$ be a new variable. Let $f_i(t) = (t - x_{\beta_i})(t - x_{\gamma_i})$ ($i = 1, 2, 3$). Our determinant vanishes if and only if $f_1, f_2, f_3$ are linearly dependent over the field $F(x_1, \ldots, x_6)$. Any of (a), (b) and (c) is clearly a sufficient condition of this.

Let now $a_1 f_1 + a_2 f_2 + a_3 f_3 = 0$ where $a_1, a_2, a_3 \in F(x_1, \ldots, x_6)$, not all zero.

Assume first $\beta_1 = \beta_2$. Then $f_1(x_{\beta_1}) = f_2(x_{\beta_1}) = 0$, hence either $a_3 = 0$, or $f_3(x_{\beta_1}) = 0$. In the latter case $\beta_1 \in \{\beta_3, \gamma_3\}$, and (b) holds. In the first case $f_1$ and $f_2$ are linearly dependent, whence $\gamma_1 = \gamma_2$ and (a) holds.

By symmetry, we may now assume that the sets $\{\beta_i, \gamma_i\}$ ($i = 1, 2, 3$) are pairwise disjoint. If moreover, $\beta_i = \gamma_i (i = 1, 2, 3)$, we have twice a non-vanishing Vandermonde determinant, consequently (c) holds.

Assume now $\beta_1 \neq \gamma_1$. Replacing $x_{\beta_1}$ at every occurrence by $x_{\beta_1}$, we obtain a vanishing determinant of the kind first treated. We conclude that either $\beta_1$ or $\beta_2$ belongs to $\{\beta_3, \gamma_3\}$, or $\gamma_1 = \gamma_2$, or if $\gamma_2 = \beta_2$ $\gamma_1 = \beta_1$. Any of these possibilities contradicts the assumptions that $\gamma_1 \neq \beta_1$ and the sets $\{\beta_i, \gamma_i\}$ are pairwise disjoint. \hfill $\Box$

**Lemma 2.3** (Atkin [1, Lemma 3]). Suppose that a non-zero polynomial $f$ in the polynomial ring $\mathbb{F}[x_1, \ldots, x_k]$ over a field $\mathbb{F}$ has degree less than the order of $\mathbb{F}$ in every single variable $x_i$. Then the function $f^*: \mathbb{F}^k \to \mathbb{F}$ defined by $f$ is not identically zero.
We shall also need an analogous lemma for an infinite set of variables. Each cardinal is, as customary, identified with its initial ordinal number. \( \beta < \kappa \) below indicates that \( \beta \) is an ordinal less than \( \kappa \).

**Lemma 2.4.** Let \( \kappa \) be an infinite cardinal, \( I \) an integral domain of power \( \geq \kappa \), \( H \) a subset of \( I \), having power less than \( \kappa \), further \( \{ \gamma_\beta : \beta < \kappa \} \) a set of variables and \( m \) an integer. Let \( \mathcal{F} \) denote the subset of the polynomial ring \( \mathbb{I}[x_\beta : \beta < \kappa] \), consisting of those non-zero polynomials having degree \( \leq m \) in every single variable \( x_\beta \), and having all coefficients from \( H \).

Then there are elements \( \xi_\beta \in I (\beta < \kappa) \) such that, \( f(\xi_\beta : \beta < \kappa) \neq 0 \) for any \( f \in \mathcal{F} \).

**Proof.** Let \( \mathcal{F}_\lambda = \mathcal{F} \cap F[x_\beta : \beta < \lambda] (\lambda < \kappa) \). We shall define \( \xi_\beta \in I \) by transfinite recursion. Assume that the following condition \((A_\lambda)\) holds:

\[ (A_\lambda) \quad \xi_\beta \text{ is defined for all } \beta < \lambda \text{ such that none of the polynomials in } \mathcal{F}_\lambda \text{ vanishes if substituting } \xi_\beta \text{ for } x_\beta (\beta < \lambda). \]

Any \( f \in \mathcal{F}_{\lambda+1} \) is a polynomial of \( x_\lambda \), with coefficients belonging to \( \mathcal{F}_\lambda \). By assumption, none of these coefficient polynomials turns into the zero polynomial if substituting \( \xi_\beta \) for \( x_\beta (\beta < \lambda) \). As \( |\mathcal{F}_\lambda| < \kappa \), it follows that there is a \( \xi_\beta \in I \) which is not a root of any of the resulting polynomials of \( x_\lambda \). This choice of \( \xi_\beta \) assures that \( A_{\lambda+1} \) is valid. For \( \lambda < \kappa \) a limit ordinal, \( A_\lambda \) clearly follows from the conditions \( A_{\mu}, \mu < \lambda \). Observing that \( A_0 \) holds, we obtain \( A_\kappa \) hence the lemma. \( \square \)

**Theorem 2.5.** Let \( k \geq 3 \) and let \( X = (V, E) \) denote a (finite or infinite) graph without loops and parallel edges. Then \( \text{St}_k(X) \) is representable over any field \( F \) of power \( |F| \geq |V|^{2k-1} \).

**Proof.** The case \( rk(\text{St}_k(X)) < k \) being obvious we assume \( rk(\text{St}_k(X)) = k \).

Let us associate distinct variables \( \{x_v : v \in V\} \) and \( \{y_{e,j} : e \in E, j = 1, 2, \ldots, k-3\} \) with the graph \( X \). First we represent the matrix \( M = M(E) = \text{St}_k(X) \) over the field \( F' = F(x_v, y_{e,j} : V \in V, e \in E, 1 \leq j \leq k-3) \). Let us associate the \( k \)-dimensional vector \( a_e = [1, x_v + x_{v', x_1, 1} y_{e,1}, \ldots, y_{e,k-3}] \) with \( e = \{v, w\} \in E \).

Let \( e_1, \ldots, e_k \) be a set of \( k \) distinct edges of \( X \). Let us consider the \( k \) by \( k \) matrix \( A = [a_{e_1}^T, \ldots, a_{e_k}^T] \) (\(^T\) indicates transpose.) Expanding the determinant of \( A \) as a polynomial of the \( y \)'s we see that the coefficient of \( \prod_{i=1}^k y_{e_i, \pi_i} \), where \( J \subseteq \{1, \ldots, k\}, |J| = k-3 \) and \( \pi \) is a bijection \( \pi : J \rightarrow \{1, \ldots, k-3\} \) is \pm a determinant of the form described in Lemma 2.2. It follows that if \( \det A = 0 \), then the edges \( e_j, j \in \{1, \ldots, k\} \setminus J \), have a vertex in common. (The other possibilities of Lemma 2.2 are excluded as the \( e_j \)'s are distinct and there are no loops in \( X \).) As this holds for any \( 3 \) edges, all the \( k \) edges \( e_1, \ldots, e_k \) have a common vertex.

On the other hand, if \( e_1, \ldots, e_k \) have a common vertex then the first \( 3 \) rows of \( A \) are linearly dependent over \( F' \) (by Lemma 2.2), hence \( \det A = 0 \).
To sum up: a $k$-tuple of edges is independent in $M$ if and only if the corresponding vectors $a_e$ are independent over $F'$. These $k$-tuples being the bases of $M$ we see that the mapping $e \mapsto a_e$ is a representation of $M$ over $F'$.

Now we use Lemmas 2.3 and 2.4 to obtain a representation of $M$ over $F$ rather than over $F'$.

Let us introduce the notation $\kappa = |V| - (k - 3) |E|$, and

$$\{x_\beta : \beta < \kappa\} = \{x_e : e \in V\} \cup \{v_{e,j} : e \in E, j = 1, \ldots, k - 3\}.$$

For $B = \{e_1, \ldots, e_k\}$ a basis of $M$, let $f_B$ denote the non-zero polynomial

$$\det A = \det [a_{e_1}^\kappa, \ldots, a_{e_k}^\kappa] \in F[x_\beta : \beta < \kappa].$$

We have to find $\xi \in F (\beta < \kappa)$ such that none of these polynomials vanish if substituting $\xi$ for $x_e$. (Such a substitution changes our representation $e \mapsto a_e$ over $F'$ into a representation $e \mapsto a_e$ over $F$.)

Let $1$ denote the unit element of $F$ and $\mathcal{H} = \{l : -6 \leq l \leq 6\}$. Clearly, all coefficients of $f_B$ belong to the finite set $\mathcal{H} \subseteq F$. Moreover, $f_B$ has degree $\leq 2$ in every single variable.

Let us first consider the case when $V$ is infinite. Clearly, $|V| = \kappa$. Assume $|F| \geq \kappa$. Then an application of Lemma 2.4 shows that the required substitution exists.

Let now $V$ be finite. Set $f = \prod f_B$ where the product is taken over all bases $B$ of $M$. The degree of $f$ in any variable $y_{e,j} (e \in E, j = 1, \ldots, k - 3)$ is at most $\binom{|E|}{k - 1}$; and in any variable $x_e (e \in V)$ it is at most $\deg v_{e,j}$. Hence, in both cases, it is less than $|V| |E|^{k-1}/(k - 1)! < |V|^{2k-1}$. An application of Lemma 2.3 completes the proof. $\square$

Remark 2.6. From the proof we obtain, for finite $V$, that

$$|F| > d_{\text{max}} \left( \frac{|E|}{k - 1} \right)$$

is sufficient, where $d_{\text{max}}$ is the maximum degree of the vertices of $X$. This is not best possible. If $X$ is an infinite graph without isolated vertices, our condition $|F| \geq |V|$ is clearly best possible.

3. Conclusions

Theorem 3.1. Given a group $G$ and an integer $k \geq 3$ there exists a matroid $M$ of rank $k$ such that

(a) $\Aut M \cong G$;

(b) any $(k - 1)$-set is independent in $M$;

(c) $M$ is representable over any field $F$ of power $|F| \geq |G|$ for infinite $G$, and of power $|F| \geq f(|G|, k)$ for finite $G$ (where the function $f(u, k)$ takes finite values).
Proof. This is a combination of Lemma 2.2 and Theorem 2.5, in view of the following result: Given a group $G$ and an integer $k$ there is a graph $X$ (without loops and parallel edges) such that $\text{Aut }X \cong G$ and every vertex of $X$ has degree $\geq k$. $X$ may be required to be finite if $G$ is finite and to have the same cardinality as $G$ if $G$ is infinite.

For finite $G$ this result is due to Frucht [3, cf. 6, p. 169]. An obvious modification of his proof is necessary to obtain degrees $\geq k$. The existence of graphs $X$ satisfying $\text{Aut }X \cong G$ for infinite $G$ was proved independently by De-Groot [5] and G. Sabidussi [10], but the exact cardinality bound was first established in the proofs of much more general results by H. Harrin, Puitr and Vopěnka (see [7, 8]). □

Remark 3.2. A bound for $f(n, 3)$ can be obtained using Frucht’s theorem [4]: Given a finite group $G$ of order $n$, there is a graph $X$, having $cn \log n$ vertices, each of degree $\geq 3$, such that $\text{Aut }X \cong G$. For such a graph, $|E| = 3|V|/2$ whence, by Remark 2.6,

$$f(n, 3) \approx Cn^2 \log^2 n,$$

($c$ and $C$ are constants.) With somewhat more effort, one can derive (using the same theorem of Frucht), that

$$f(n, k) \approx (Cn \log n)^{k-1}.$$

Theorem 3.2. Given an integer $k \geq 3$, a set $S$ and a function $G : 2^S \to \text{Groups}$, associating a group with each subset of $S$, there is a matroid $M = M(E)$ such that

(i) $E \supseteq S$;
(ii) $\text{rank } M = \text{rank } (M \setminus S) = k$;
(iii) $\text{Aut } (M \setminus T) \cong G(T)$ for any $T \subseteq S$;
(iv) $M$ is representable over any sufficiently large field.

Sufficiently large means: $\geq n_0(G, k)$ where $n_0(G, k)$ is finite if $S$ and all groups in the range of $G$ are finite; and $n_0(G, k) = \sum_{T \subseteq S} |G(T)|$ otherwise. (If we require (iii) for a subset $L$ of $2^S$ only, then the infinite case, $n_0 = |S| + \sum_{T \subseteq L} |G(T)|$.)

Proof. Let $X = (V, E)$ be a graph and $T \subseteq E$. We observe that $S_k(V, E \setminus T) = S_k(X \setminus T)$ Hence, this result is a combination of Lemma 2.1, Theorem 2.5 and a result of the author [2]; a particular case of which is as follows: ($[W]^2$ denotes the set of unordered pairs from $W$.)

Given a set $W$ and a function $G$ associating a group $G(T)$ with each $T \subseteq [W]^2$, there exists a graph $X = (V, E)$ such that

(i) $V \supseteq W, E \supseteq [W]^2$;
(ii) $\text{Aut } (V, E \setminus T) \cong G(T)$ for any $T \subseteq [W]^2$;
(iii) $|V|$ is finite if $W$ and all groups in the range of $G$ are finite; $|V| = \sum_T |G(T)|$ otherwise.
It is easily seen, that one can additionally require each vertex in $(V, E \setminus \{W\})$ to have degree $\geq k$. Namely, one can join each point of $X$ to all points of an asymmetric graph $Y$ (having no non-trivial automorphism) (cf. Frucht [3]) whose vertices have degree $\geq k$. The new graph will satisfy (i), (ii), (iii) again, provided the complements of both $X$ and $Y$ are connected, which we may assume. □

4. Matroids of rank $\leq 2$

We note, that the rank condition $k \geq 3$ is necessary. The matroids of rank $\leq 2$ have an obvious structure: if $rk(M(S)) = 2$, then $M(S)$ is uniquely determined by the partition $S = S_0 \cup \{T_\alpha : \alpha \in I\}$ where $S_0$ consists of those points $x$ for which $\{x\}$ is not independent; and the $T_\alpha$'s are the classes of the equivalence relation defined on $S \setminus S_0$ by

\[ x \sim y \text{ if the family } \{x, y\} \text{ is not independent} \]

($I$ is a set of indices.)

If $|S_0| = a$, and the cardinal $b$ appears $c_b$ times as $|T_\alpha| (\alpha \in I)$, then obviously

\[ \text{Aut}(M(S)) = S_a \times \prod_b (S_b \sim S_{c_b}) \]

where $S_n$ denotes the symmetric group of degree $n$, and $\sim$ indicates wreath product. ($a, b, c_b$ may be infinite.)

References

[9] E. Mendelsohn, Every group is the collineation group of some projective plane, J. Geometry 2(1972) 97-106.