DISCRETE MATHEMATICS 2 (1972) 163–171. North-Holland Publishing Company

ON THE AUTOMORPHISM GROUP OF A MATROID

F. HARARY

Department of Mathematics, University of Michigan, Ann Arbor, Mich. 48104, U.S.A.

M.J. PIFF and D.J.A. WELSH

Mathematical Institute, University of Oxford, 24-29 St. Giles, Oxford, OX1 3LB, England

Received 20 October 1970*

Abstract. We show that for any group H (finite or infinite) there exists an independence structure with automorphism group isomorphic to H. The proof is by construction and shows that for any H there is a geometric lattice with automorphism group isomorphic to H.

§ 1 Introduction

We show that for any group H (finite or infinite) there exists an independence structure with automorphism group isomorphic to H. The proof is by construction and shows that for any H there is a geometric lattice with automorphism group isomorphic to H.

An *independence structure* on a set S is a family $\mathcal{I}$ of subsets of S such that:

(i) $\emptyset \in \mathcal{I}$.

(ii) If $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$.

(iii) If $A \in \mathcal{I}$ and $B \in \mathcal{I}$ with $|A| = |B| + 1$, there exists $a \in A - B$ such that $B \cup \{a\} \in \mathcal{I}$.

(iv) $\mathcal{I}$ has *finite character*, that is if X is an infinite subset of S and every finite subset $Y \subset X$ also belongs to $\mathcal{I}$, then $X \in \mathcal{I}$.

When S is finite, the independence structure is a *matroid* M on S. The members of $\mathcal{I}$ are called *independent sets*. A *base* is a maximal independent set. Another matroidal teminology is that of [4] and apart from the existence of a dual it carries over to independence structures in the obvious way.

* Revised version received 21 April 1971; final version received 16 August 1971.

A permutation ϕ of S *preserves incidence* provided $X \in \mathcal{I}$ if and only if $\phi(X) \in \mathcal{I}$. The *automorphism group* of an independence structure $\mathcal{I}$ is the collection of permutations of S which preserve independence, and will be denoted by $A(\mathcal{I})$, or by $A(M)$ when the structure is a matroid M.

The graph theory terminology is fairly standard, see [3].

Theorem 1. *Given any group H there exists an independence structure $\mathcal{I}$ such that the automorphism group of $\mathcal{I}$ is isomorphic to H.*

From the proof, it will be clear that when the group H is finite, we can find a matroid M such that the automorphism group of M is isomorphic to H.

§ 2. Proof of the main theorem

To prove Theorem 1, we need the following lemmas about infinite graphs.

A *graph* G consists of a set $V = V(G)$ (possibly infinite) of vertices and a subset $E = E(G)$ of edges, that is, of unordered pairs $[u, v]$ of distinct vertices. A *cycle* in G is a finite sequence of edges $[v_1, v_2]$ $[v_2, v_3]$ ... $[v_{n-1}, v_n]$ $[v_n, v_1]$, where v_i $(1 \leq i \leq n)$ are distinct elements of V. If we let $X \subset E$ be a member of $M(G)$ if and only if X does not contain a cycle, then it is easily seen (Piff [6]) that $M(G)$ is an independence structure on E. In the case where G is finite, $M(G)$ is just the cycle matroid of G; see [3]. Let $A_p(G)$ be the *point automorphism group* of G, and let $A_c(G)$ be the *cycle automorphism group* of G. That is, a permutation π of V is a member of $A_p(G)$ provided $[v_1, v_2] \in E(G)$ if and only if $[\pi(v_1), \pi(v_2)] \in E(G)$. A permutation ϕ of E is a member of $A_c(G)$ if a subset X is a cycle of G if and only if $\phi(X)$ is also a cycle of G.

Lemma 1. $A_c(G) = A(M(G))$.

We omit the proof, which is obvious from the definition.

Lemma 2. *If G is 3-connected, then $A_p(G) \cong A_c(G)$.*

Proof. In the finite case, the theorem is essentially proved by Whitney [9]; see [5, Theorem 15.4.4.].

Let G be 3-connected and infinite. As in the finite case, call a subset X of $E(G)$ a *cocycle* of G it it is a minimal disconnecting set of edges of G. In general, independence structures do not have duals in the same way as matroids. However, analogous to the finite case, it is true that X is a cocycle of G if and only if X has a non-null intersection with every spanning tree of G, that is, with every base of $M(G)$, and X is minimal with respect to this property. Alternatively, we can prove that a cocycle of G is the complement in $E(G)$ of some hyperplane (maximal proper closed set) of $M(G)$. Now if $\phi \in A_c(G)$, then $\phi \in A(M(G))$ and hence ϕ preserves hyperplanes of $M(G)$. Thus ϕ preserves cocycles of G.

If $v \in V(G)$, let st(v), the *star* at v, be the set of edges of G incident with v. Then st(v) is a cocycle of G since G is 3-connected. If $e_1, e_2 \in E - \mathrm{st}(v)$, since G is 3-connected, $G - \mathrm{st}(v)$ is at least 2-connected and hence there exists a cycle $C \subset E(G) - \mathrm{st}(v)$ such that $\{e_1, e_2\} \subset C$. Thus

$$\phi(\{e_1, e_2\}) \subset \phi(C) \subset E - \phi(\mathrm{st}(v)).$$

Thus the removal of $\phi(\mathrm{st}(v))$ from $E(G)$ results in a graph G' in which any pair of edges is contained in a cycle and therefore, since also $\phi(\mathrm{st}(v))$ is a cocycle, this can only happen if there exists some vertex $v' \in V(G)$ such that $\phi(\mathrm{st}(v)) = \mathrm{st}(v')$.

Define the map Ψ: $V(G) \to V(G)$ by $\Psi(v) = v'$. This is clearly a bijection, and if there exists an edge $[v_1, v_2] \in E(G)$, then $\phi(\mathrm{st}(v_1)) \cap \phi(\mathrm{st}(v_2)) \neq \emptyset$, hence $[\Psi(v_1), \Psi(v_2)] \in E(G)$ and $\Psi \in A_p(G)$. It is trivially verified that the map f: $A_c(G) \to A_p(G)$ defined by $f(\phi) = \Psi$ is a group isomorphism, thus completing the proof of Lemma 2.

In [8], Sabidussi proves:

Lemma 3. *Given a group H, there exists a graph G such that H is isomorphic to $A_p(G)$.*

The graph so constructed in [8] is however only 1-connected and $A_p(G) \not\cong A_c(G)$.

Lemma 4. *For any positive integer ρ and finite group H, there exists a finite ρ-connected graph G with $A_p(G) \cong H$.*

This is proved in Sabidussi [7].

For the proof of Theorem 1 and Corollary 1 we need a 3-connected graph with given group H.

Lemma 5. *For any positive integer ρ and group H, there exists an infinite ρ-connected graph G with $A_p(G) \cong H$.*

Proof. By [8], there exist non-isomorphic 1-connected graphs G_1, $G_2, \ldots, G_\rho$ such that $A_p(G_1) \cong H$ and $A_p(G_2) = \ldots = A_p(G_\rho) = 1$. Since the G_i's are 1-connected, they are prime relative to cartesian multiplication. Hence by [7, Lemma 2.3.], $G = G_1 \times G_2 \times \ldots \times G_\rho$ is ρ-connected and by [7, Lemma 2.10.].

$$A_p(G) \cong A_p(G_1) \times A_p(G_2) \times \ldots \times A_p(G_\rho) \cong H.$$

This is really all that is needed for the proof of Theorem 1!

We can now complete the proof of Theorem 1. By Lemma 5, for any group H there is a 3-connected graph G such that $A_p(G) \cong H$. By Lemma 2, $A_p(G) \cong A_c(G)$, and by Lemma 1, $M(G)$ has automorphism group isomorphic to H.

Corollary 1. *Given any group H there exists an independence structure $\mathcal{I}$ such that all the following properties hold:*

(i) $A(\mathcal{I}) \cong H$,

(ii) *$\mathcal{I}$ is a geometry,*

(iii) *$\mathcal{I}$ is graphic,*

(iv) *$\mathcal{I}$ is non-separable,*

(v) *$\mathcal{I}$ is a non-transversal structure.*

Proof. The only statement not immediately obvious from the proof of Theorem 1 is (v). Every 3-connected graph without parallel edges contains K_4 as a homeomorph (perhaps this is a well-known result). For suppose G is 3-connected and $[v_1, v_2]$ is an edge of G. Let p_1, p_2 be paths joining v_1 and v_2 in G disjoint from $[v_1, v_2]$, and suppose v_3 and v_4 are intermediate nodes on p_1 and p_2, respectively. Then, since G is 3-connected, there exists a path p_3 from v_3 to v_4 which does not pass through v_1 or v_2. Let v_5 be the last vertex of $p_1 \cap p_3$ and v_6 the following vertex of $p_2 \cap p_3$. Put p_4 equal to the section of p_3 joining v_5 and v_6. The the subgraph consisting of $[v_1, v_2], p_1, p_2$ and p_4 is a homeomorph of K_4.

Taking a 3-connected graph G with $A_p(G) \cong H$, we see that G contains K_4 as a homeomorph, hence, by a recent result of Bondy [2], $M(G)$ is not transversal.

From (ii) and the correspondence between geometries and geometric lattices (semimodular, relatively complemented, atomic, and of finite length), we have:

Corollary 2. *Given any group H, there exists a geometric lattice with automorphism group isomorphic to H.*

This result neither implies nor is implied by the theorem of Birkhoff [1] who shows the existence of a distributive lattice with arbitrary automorphism group.

§ 3. The infinite version of Lemma 5

The strong infinite version of Lemma 5 is of independent interest and is now demonstrated.

Theorem 2. *For any cardinal $\rho > 0$ and infinite group H, there exists an infinite ρ-connected graph G with $A_p(G) \cong H$.*

Proof. Let G_1 and G_2 be edge- and vertex-disjoint, 1-connected graphs such that $A_p(G_2) \cong H$ and $A_p(G_1)$ is the identity group, and such that $|V(G_1)| > \rho$, $|V(G_1)|$ is infinite. Let $V(G_1) = V_1 = \{v_i : i \in I\}$ and $V(G_2) = V_2 = \{v_j : j \in J\}$. Let $V = \{v_{ij} : i \in I, j \in J\}$ be a set disjoint from V_1 and V_2. Let G' be a graph with vertex set $V_1 \cup V_2 \cup V$, such that $G' - (V_1 \cup V) = G_2$, $G' - (V_2 \cup V) = G_1$. Also for each $i \in I, j \in J$, let there be edges in G' joining v_{ij} to v_i and v_j. Thus in G', if $v \in V_1 \cup V_2$, then v has degree strictly greater than ρ, and if $v \in V$, then v has degree 2.

Let u, v denote two arbitrary vertices of G'. If $\{u, v\} \subset V_1$ or if $\{u, v\} \subset V_2$, there exist at least ρ vertex-disjoint paths from u to v in G'. If $u \in V_2$, $v \in V_1$, we find ρ vertex-disjoint paths in G' from u to v as follows. There is one path of length 2. There are $\rho - 1$ paths of length 2 from u into $V_1 - v$, followed by $\rho - 1$ disjoint paths returning from $V_1 - v$ to $V_2 - u$, and finally $\rho - 1$ paths from $V_2 - u$ to v.

Since $A_p(G_2) \cong H$ and H is infinite, $|V_2| = \infty$ and since V_1 is infinite and $> \rho$, we can partition V_1 into disjoint $(\rho - 1)$-subsets, say $(A_k : k \in K)$. For each $k \in K$ and $v_{j_0} \in V_2$, if $A_k = \{v_i : i \in I_k\}$, we form the complete graph with vertex set $\{v_{ij_0} : i \in I_k\}$. Denote this graph by $G(k, j_0)$. Now let $G = G' \cup \bigcup_{k, j_0} G(k, j_0)$. We claim that G is ρ-connected and $A_p(G) \cong H$. There are several cases to consider. We list in each case ρ disjoint paths connecting two arbitrary vertices u and v, and throughout this listing will often refer to "paths" when we mean "collection of vertex-disjoint paths".

Case 1. There exist k, j_0 such that $\{u, v\} \subset G(k, j_0)$. It is trivial that ρ disjoint paths exist.

Case 2. $u \in G(k_1, j_0)$, $v \in G(k_2, j_0)$, where $k_1 \neq k_2$. There is a path (u, v_{j_0}, v) and $\rho - 1$ additional paths obtained by connecting $\rho - 1$ paths from u to A_{k_1} to the $\rho - 1$ paths of length 4 from A_{k_1} to A_{k_2} and then connecting the $\rho - 1$ paths from A_{k_2} to v.

Case 3. $u \in G(k, j_0)$, $v \in G(k, j_1)$. There are $\rho - 1$ paths from u to A_k and $\rho - 1$ paths from A_k to v. There is a further disjoint path from u to v through v_{j_0} and v_{j_1}.

Case 4. $u \in G(k_1, j_1)$, $v \in G(k_2, j_2)$, where $k_1 \neq k_2$, $j_1 \neq j_2$. There is one path P_1 from A_{k_1} to A_{k_2} which only intersects A_{k_1} and A_{k_2} at its endpoints and otherwise lies in G_2. Letting u_1, v_1 be the endpoints of P we have a path u, u_1, P, v_1, v. Now consider the $\rho - 2$ paths of length 4 from $A_{k_1} - u_1$ to $A_{k_2} - v_1$ which pass through $V_2 - v_{j_1} - v_{j_2}$. These can be extended to paths from u to v. Finally, it is easy to see that there is a path Q of length 4 from v_{j_1} to v_{j_2} such that $Q \cap P = Q \cap A_{k_1} = Q \cap A_{k_2} = \emptyset$. The path $u\, v_{j_1} Q v_{j_2} v$ is a path disjoint from the $\rho - 1$ previously constructed.

Case 5. $u \in G(k, j_0)$, $v = v_{j_0}$. In this case, $\rho - 1$ disjoint paths are immediately obvious. The last is obtained by taking the edge from u to A_k followed by a path in G_1 to a vertex outside A_k and then a path of length 2 to $v_{j_0} = v$.

Case 6. $u \in G(k, j_0)$, $v = v_{j_1}$, $j_1 \neq j_0$. There exist $\rho - 1$ disjoint paths from u through $G(k, j_0)$ to A_k. To these connect the $\rho - 1$ disjoint paths from A_k through $G(k, j_1)$ to $v_{j_1} = v$. Also there is a path disjoint from these of the form $u v_{j_0} Q$ where Q is a path from v_{j_0} to v_{j_1} contained in G_2.

Case 7. $u \in G(k, j_0)$, $v \in A_k$. There is a path of length at most 2 from u to v. There is a second from u to v_{j_0} to v_{j_1} ($j_1 \neq j_0$) and then two further edges across to v. The remaining $\rho - 2$ paths are obtained by travelling along $\rho - 2$ paths through $G(k, j_0)$ to A_k, then across to $\rho - 2$ distinct points in $G_1 - v_{j_0} - v_{j_1}$, followed by $\rho - 2$ paths to v.

Case 8. $u \in G(k, j_0)$, $v \in G_2 - A_k$. This is very similar to case 7 and clear from a diagram.

As these eight cases are exhaustive, this completes the proof that G is ρ-connected. Now consider any $\phi \in A_p(G)$. Clearly ϕ must map V onto itself from vertex degree arguments. Consider $G - V$ and $\phi' = \phi$ restricted to $G - V$. Then ϕ' must be an automorphism of $G - V$. Since G_1 and G_2 are connected components of $G - V$, we have $\phi'(V_1) = V_1$ and $\phi'(V_2) = V_2$. Hence since $A_p(G_1)$ is the identity group, ϕ' and thus ϕ restricted to G_1 must be the identitiy; therefore ϕ is uniquely determined by its effect on G_2. That is, $A_p(G) \cong A_p(G_2) \cong H$, which proves the theorem.

§ 4. Further results

A trivial but useful result is the following:

Theorem 3. *For any matroid M on S and its dual M^*, $A(M^*) = A(M)$.*

Proof. Obvious since the dual is unique.

Theorem 4. *A matroid M on a set of cardinality n has S_n as its automorphism group if and only if M has as bases every k-subset of S for some k, $1 \leq k \leq n$, i.e., is k-uniform.*

Proof. Let $A(M) = S_n$. Let M have rank r. Take any base B. For any r-set $X \in S$, there exists $\pi \in A(M)$ such that $\pi(B) = X$. Hence every r-set in S must be independent.

Theorem 5. *An independence structure I on an infinite set S has the full permutation group as its automorphism group if and only if either (a) it is k-uniform for some finite k or (b) it is the trivial structure in which every subset of S is independent.*

The proof is very similar to that of Theorem 4 and will be omitted.

Theorem 6. *There is no matroid on a set of n elements with automorphism group equal to the alternating group A_n for any $n \geq 3$.*

Proof. Let $n \geq 3$. It is well-known that A_n is $(n-2)$-ply transitive. Hence suppose $A(M) = A_n$ and M has rank $r \leq n-2$. Then every r-subset of S is independent and hence $A(M) = S_n$. If M has rank $> n-2$, then M^* has rank $\leq n-2$ and so $A(M^*) = S_n$, whence by Theorem 3, $A(M) = S_n$.

An interesting application of the above theory is as follows. Consider the 3-dimensional Desargues configuration. Regarded as a matroid with independence induced by projective independence, it has rank 4 on a set of 10 elements and is easily seen to be the same matroid as the cycle matroid of K_5. Hence its automorphism group is the same as the automorphism group of $M(K_5)$. Also since K_5 is 3-connected,

$A(M(K_5)) \cong A_p(K_5) = S_5$, and we see that the Desargues configuration has automorphism group isomorphic to S_5.

References

[1] G. Birkhoff, On groups of automorphisms, Rev. Un. Mat. Argentina 11 (1946) 155–157.
[2] J.A. Bondy, Transversal matroids, base orderable matroids and graphs, J. London Math. Soc., to appear.
[3] F. Harary, Graph theory (Addison-Wesley, Reading, Mass., 1969).
[4] F. Harary and D.J.A. Welsh, Matroids versus graphs, in: G. Chartrand and S.F. Kapoor, eds., The many facets of graph theory (Springer, New York, 1969) 155–170.
[5] O. Ore, Theory of graphs (Am. Math. Soc. Colloq. Publ., Providence, 1962).
[6] M.J. Piff, Properties of finite character of independence spaces, to appear.
[7] G. Sabidussi, Graphs with given group and given graph-theoretical properties, Canad. J. Math. 9 (1957) 515–525.
[8] G. Sabidussi, Graphs with given infinite group, Monatsh. Math. 64 (1960) 64–67.
[9] H. Whitney, Congruent graphs and the connectivity of graphs, Am. J. Math. 54 (1932) 150–168.