INVOLUTIONS OF CONNECTED BINARY MATROIDS

JOSEPH E. BONIN

ABSTRACT. We prove that if an involution ϕ is an automorphism of a connected binary matroid M, then there is a hyperplane of M that is invariant under ϕ. We also consider extensions of this result for higher connectivity.

1. THE MAIN RESULT

Is any substructure of a matroid necessarily invariant under any automorphism? The answer, in general, is no. In contrast, we show that by focusing on connected binary matroids and requiring that the automorphism ϕ be an involution (i.e., ϕ^2 is the identity map), then there is at least one hyperplane H with $\phi(H) = H$. It follows that there is also at least one invariant cocircuit and, by duality, at least one invariant circuit.

We are concerned with matroid automorphisms that are also involutions; for brevity, we simply refer to such maps as involutions. In addition to the standard terminology and notation of matroid theory (see, e.g., [1]), we use $C_B(x)$ to denote the fundamental circuit of an element x with respect to a basis B.

Our main result is Theorem 1.1. The special case for 2-connected graphs was proven by Sjogren [2].

Theorem 1.1. *Let ϕ be an involution of a connected binary matroid M with at least two elements. There is a hyperplane H of M with $\phi(H) = H$.*

Before proving this result, we note the necessity of the hypotheses. Three of the involutions of the four-point line, $U_{2,4}$, have no fixed points and so have no invariant hyperplanes. (One can generalize this example.) Thus Theorem 1.1 cannot be extended beyond the class of binary matroids. The assumption that M is connected is also essential: if N_1 and N_2 are isomorphic matroids on disjoint sets with $\psi : N_1 \to N_2$ an isomorphism, then the map $\phi : N_1 \oplus N_2 \to N_1 \oplus N_2$ that takes each element in N_i, $i = 1, 2$, to its image or preimage under ψ is an involution with no invariant hyperplanes.

Proof of Theorem 1.1. Since M is connected and ϕ maps parallel classes to parallel classes, there is no loss of generality in assuming M is simple. Build a chain of invariant flats in M as follows. The least flat $X_0 = \emptyset$ is invariant. Pick an element x_1. If $\phi(x_1) = x_1$, we have an invariant point; otherwise the line $\text{cl}(\{x_1, \phi(x_1)\})$ is invariant. In general, given an invariant flat X_i, pick x_{i+1} not in X_i; the flat $X_{i+1} = \text{cl}(X_i \cup \{x_{i+1}, \phi(x_{i+1})\})$ is invariant. This construction results in a chain $X_0, X_1, \dots, X_t$ of flats with these properties: each X_i is invariant under ϕ; each increase in rank, $r(X_{i+1}) - r(X_i)$, is 1 or 2; and X_t is M. Note also that the construction yields a basis for each of these flats; if $r(X_{i+1}) - r(X_i) = 2$, both x_{i+1} and $\phi(x_{i+1})$ are in the basis for X_{i+1} and the later flats in the chain, otherwise only x_{i+1} is in these bases.

We claim that if any difference in ranks, $r(X_{i+1}) - r(X_i)$, is 1, then there is an invariant hyperplane. To see this, let i be the largest integer for which $r(X_{i+1}) - r(X_i)$ is 1. Therefore there is a basis B for $X_t = M$ consisting of a basis of the invariant flat X_i, along with x_{i+1}, and pairs of elements $x_{i+2}, \phi(x_{i+2}), x_{i+3}, \phi(x_{i+3}), \ldots, x_t, \phi(x_t)$. Thus $B - \{x_{i+1}\}$ spans an invariant hyperplane.

It follows easily from this that if there is an invariant flat of odd rank, then there is an invariant hyperplane.

We now use the assumptions that M is connected and binary. By the work above, we may assume that the rank is even, say $2k$, that ϕ has no fixed points, and that M has an invariant basis. Under a coordinatization of M over $GF(2)$, we may assume that the standard basis $B = \{e_1, e_2, \ldots, e_{2k}\}$ is a basis of M with $\phi(B) = B$. Let S denote the ground set of M. With each element v of $S - B$ we have its fundamental circuit, $C_B(v)$; indeed, under the coordinatization of M, we have $v = \sum_{e_i \in C_B(v)} e_i$, or $\sum_{x \in C_B(v)} x = 0$. The following observation justifies all invariance assertions below: for $v \in S - B$, we have $\phi(C_B(v)) = C_B(\phi(v))$. Let Γ be the graph with vertex set $S - B$ and with an edge joining the pair $v, u \in S - B$ whenever $C_B(v) \cap C_B(u) \neq \emptyset$. It is easy to show that Γ is connected.

The involution ϕ of M induces an involution of Γ that has no fixed vertices. Furthermore, we may assume there are no invariant edges in Γ, for if vertices v and $\phi(v)$ are adjacent in Γ, then there is an invariant flat of odd rank. Indeed, if $C_B(v) \cap C_B(\phi(v)) \neq \emptyset$, it follows that the symmetric difference $C_B(v) \triangle C_B(\phi(v))$ is an invariant circuit of M of even cardinality and hence spans an invariant flat of odd rank.

Since Γ is connected and there are neither invariant vertices nor invariant edges, the distance $d(v, \phi(v))$ between each vertex and its image is at least two. Let $v_0, \phi(v_0)$ be a pair for which $d(v, \phi(v))$ is as small as possible, and let

$$v_0, v_1, v_2, \ldots, v_{d-1}, \phi(v_0)$$

be a shortest path connecting these vertices. It follows that

$$v_0, v_1, v_2, \ldots, v_{d-1}, \phi(v_0), \phi(v_1), \phi(v_2), \ldots, \phi(v_{d-1}), v_0$$

is a cycle of Γ and this cycle has no chords. It then follows that the symmetric difference

$$C_B(v_0) \triangle C_B(v_1) \triangle \cdots \triangle C_B(v_{d-1}) \triangle C_B(\phi(v_0)) \triangle C_B(\phi(v_1)) \triangle \cdots \triangle C_B(\phi(v_{d-1}))$$

is an invariant circuit of M of even cardinality. Therefore this circuit spans an invariant flat of odd rank, completing the proof. □

2. Further Observations

There are several natural potential extensions of Theorem 1.1 that one could investigate. We discuss several in this section.

One can ask: If the binary matroid satisfies higher connectivity properties, will there necessarily be an invariant hyperplane H so that the restriction $M|H$ is connected? That this need not be true for 3-connectivity can be seen from the cycle matroid of the complete graph on an even number of vertices, $M(K_{2t})$. Assume that $t \geq 2$ and that ϕ' is an involution of the vertex set $\{v_1, v_2, \ldots, v_{2t}\}$ of K_{2t} that has no fixed points. Note that ϕ' induces an involution ϕ of the cycle matroid $M(K_{2t})$. Hyperplanes of $M(K_{2t})$ correspond to partitions of $\{v_1, v_2, \ldots, v_{2t}\}$ into two nonempty classes, and invariant hyperplanes correspond to partitions in which the two blocks are invariant or switched under ϕ'. Since ϕ' has no fixed points, neither block in an invariant hyperplane is a singleton, so no invariant hyperplane is connected.

One can also ask whether there is necessarily more than one invariant hyperplane. For this, consider the dual property, namely having invariant circuits. The wheel $\mathcal{W}_{2t}$ with an even number of spokes shows that 3-connectivity is not enough to guarantee more than one invariant circuit. Consider a geometric realization of the wheel $\mathcal{W}_{2t}$ having as rim vertices and rim edges the vertices and edges of a regular $(2t)$-gon; each rim vertex is also joined by an edge (a spoke) to the hub vertex at the center of the $(2t)$-gon. Rotation by a half-turn around the center defines an involution, and the only circuit fixed by this involution is that formed by all rim edges.

The involution of the wheel $\mathcal{W}_{2t}$ defined by a half-turn also shows that the involution need not have fixed points. In particular, one cannot in general deduce the existence of a saturated chain of invariant flats.

Connectivity higher than three allows us to conclude more, as the next theorem states.

Theorem 2.1. *Let ϕ be an involution of a binary matroid M that is $(2k)$-connected and has at least $4k-2$ elements. There are at least k invariant hyperplanes of M.*

Proof. We treat the dual problem, namely that there are at least k invariant circuits. We induct on k. Theorem 1.1 is the base case, $k = 1$. Assume that M is $(2k)$-connected, $k > 1$, and that ϕ is an involution of M. By Theorem 1.1, since M is connected there is a circuit C of M that is invariant under ϕ. Fix $a \in C$. If $\phi(a) = a$, let M' be the deletion $M\backslash\{a\}$, otherwise let $M' = M\backslash\{a, \phi(a)\}$. By [1, Proposition 8.1.13], M' is $\big(2(k-1)\big)$-connected. By induction, M' has at least $k-1$ invariant circuits. These together with C give at least k invariant circuits of M. □

Acknowledgement

The author thanks Geoff Whittle for useful comments that influenced the second section of the paper.

References

[1] J. G. Oxley, *Matroid Theory*, (Oxford University Press, Oxford, 1992).
[2] J. A. Sjogren, Machine proof of results on connectivity, (1996) manuscript.

DEPARTMENT OF MATHEMATICS, THE GEORGE WASHINGTON UNIVERSITY, WASHINGTON, D.C. 20052