DETERMINING A BINARY MATROID FROM ITS SMALL CIRCUITS

JAMES OXLEY, CHARLES SEMPLE, AND GEOFF WHITTLE

Abstract. It is well known that a rank-r matroid M is uniquely determined by its circuits of size at most r. This paper proves that if M is binary and $r \geq 3$, then M is uniquely determined by its circuits of size at most $r-1$ unless M is a binary spike or a special restriction thereof. In the exceptional cases, M is determined up to isomorphism.

1. Introduction

A matroid M *uses* an element e or a set X if $e \in E(M)$ or $X \subseteq E(M)$. Suppose M is non-binary. Bixby [2] showed that if M is 2-connected and and $e \in E(M)$, then M has a $U_{2,4}$-minor using e. Later, Seymour [7] showed that if M is 3-connected and $e, f \in E(M)$, then M has a $U_{2,4}$-minor using $\{e, f\}$. In addition, he conjectured that if M is 4-connected and $e, f, g \in E(M)$, then M has a $U_{2,4}$-minor using $\{e, f, g\}$. Kahn [4] and Coullard [3] gave counterexamples to this conjecture leaving open the problem of characterising all 4-connected non-binary matroids that have a 3-element set that is not used by any $U_{2,4}$-minor (see [6, Problem 15.9.7]).

A rich class of counterexamples to Seymour's conjecture is provided by frame matroids with at least three joints e, f, and g. It is readily checked that, in this case, no circuit contains e, f, and g, and hence, such matroids have no $U_{2,4}$-minor using $\{e, f, g\}$. A refinement of Seymour's conjecture is to conjecture that if a matroid M is 4-connected, $e, f, g \in E(M)$, and M has a circuit containing e, f, and g, then M has a $U_{2,4}$-minor using $\{e, f, g\}$. However, this conjecture is also false. Counterexamples are given by Kahn [4] and Coullard [3]. Their counterexamples are obtained from binary matroids by relaxing circuit-hyperplanes and, indeed, the only known counterexamples to the modified version of Seymour's conjecture are obtained from binary matroids by relaxing circuit-hyperplanes; Kahn's counterexample relaxes a single circuit-hyperplane; Coullard's example relaxes

Date: December 23, 2015.

1991 *Mathematics Subject Classification.* 05B35.

Key words and phrases. Binary matroids, circuit-hyperplane relaxations.

The second and third authors were supported by the New Zealand Marsden Fund.

two circuit-hyperplanes. As a possible approach to solving the modified version of Seymour's conjecture, this paper considers the problem of whether a binary matroid M is uniquely determined by a matroid obtained from M by a sequence of circuit-hyperplane relaxations.

Let J_r and $\mathbf{1}$ be the $r \times r$ and $r \times 1$ matrices of all ones. For $r \geq 3$, let A_r be the $r \times (2r+1)$ matrix $[I_r|J_r - I_r|\mathbf{1}]$ over $GF(2)$ whose columns are labelled, in order, $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_r, t$. The vector matroid $M[A_r]$ of this matrix is called the *rank-r binary spike with tip t*. For each i in $\{1, 2, \ldots, r\}$, the set $\{t, x_i, y_i\}$ is a triangle of $M[A_r]$. We call $\{t, x_1, y_1\}, \{t, x_2, y_2\}, \ldots, \{t, x_r, y_r\}$ the *legs* of $M[A_r]$. The matroid $M[A_r]\backslash t$ is called the *rank-r tipless binary spike*. Its *legs* are the sets $\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_r, y_r\}$. Throughout this paper, we will use the term *binary spike* to include binary spikes with tips as well as tipless binary spikes.

The following is the main result of the paper. As we shall see, most of the effort in proving this result is devoted to verifying the last sentence.

Theorem 1.1. *For $r \geq 3$, let M be a rank-r binary matroid on a given ground set, and suppose that $\mathrm{si}(M)$ is not isomorphic to $U_{r-1,r} \oplus U_{1,1}$ or $U_{r,r+1}$. Then M is uniquely determined by its circuits of size at most $r-1$ unless $\mathrm{si}(M)$ is isomorphic to $M(K_{3,2})$ or can be obtained from a binary spike by deleting at most $r-1$ elements no two of which belong to the same leg. In the exceptional cases, M is uniquely determined up to isomorphism.*

Let M be a rank-r binary spike with r in $\{3, 4\}$. If $r = 3$ and M has a tip, then any set of three lines through a common point can be chosen as the legs of the spike. If $r = 4$ and M is tipless, then $M \cong AG(3, 2)$ and again there are seven different choices for the sets of legs. In these, the only two, cases where there are choices for the sets of legs, the assertion in the theorem that the deleted elements can all be chosen from different legs means that there is a choice of legs for which this is true rather than that this is true for all choices of the legs.

For arbitrary r exceeding 2, consider $M[A_r]$, the binary spike with tip. Let i be an element of $\{1, 2, \ldots, r\}$ and let $\{u_i, v_i\} = \{x_i, y_i\}$. It is well known [5, p.66] and easily checked that the dual of $M[A_r]\backslash u_i, t$ is isomorphic to the rank-$(r-1)$ binary spike with tip v_i. In each of $M[A_r]\backslash t, u_i$ and $M[A_r]\backslash u_i$, we call v_i the *cotip*. The last two matroids, which are well known to be unique up to isomorphism, are called, respectively, the *rank-r binary spike with a cotip and no tip*, and the *rank-r binary spike with a tip and a cotip*.

Theorem 1.1 is a strengthening, for binary matroids, of the well-known fact that an arbitrary matroid is uniquely determined by its non-spanning circuits. Observe that, unless $n = 1$ or $n = 2$, an n-element rank-1 or rank-2

binary matroid is not uniquely determined by its set of circuits of size zero or size at most one, respectively. Also, for $r \geq 3$, the sets of circuits of size at most $r-1$ are the same in $U_{r,r+1}$ and $U_{r-1,r} \oplus U_{1,1}$. Moreover, for all $r \geq 4$, no rank-r binary spike is uniquely determined by its circuits of size at most $r-1$. To see this, fix $r \geq 4$, and let M_1 and M_2 be two rank-r binary spikes with tip t and legs $\{t, x_1, y_1\}, \{t, x_2, y_2\}, \ldots, \{t, x_r, y_r\}$ with the property that $\{x_1, x_2, \ldots, x_r\}$ is a basis of M_1 and $\{x_1, x_2, \ldots, x_{r-1}, y_r\}$ is a basis of M_2. Since M_1 and M_2 are binary, $\{x_1, x_2, \ldots, x_{r-1}, y_r\}$ is a circuit-hyperplane of M_1, and $\{x_1, x_2, \ldots, x_r\}$ is a circuit-hyperplane of M_2. Hence $M_1 \neq M_2$, but M_1 and M_2 have the same sets of circuits of size at most $r-1$. Note that, for all $r \geq 4$, we see the same phenomenon when M_1 and M_2 are both spikes without tips, or are both spikes with tips and cotips, or are both tipless spikes with cotips. However, these exceptions can be eliminated when $r \geq 5$ if we know at least one circuit of size r or $r+1$.

Theorem 1.2. *For $r \geq 5$, let M be a rank-r binary matroid on a given ground set. Let C^+ be a fixed circuit of M choosing $|C^+| \geq r$ if possible. Then M is uniquely determined by the collection*

$$\{C : C \in \mathcal{C}(M) \text{ and } |C| \leq r-1\} \cup \{C^+\}.$$

Note that $M(K_4)$ and $M(K_{3,2})$ show that Theorem 1.2 cannot be extended to allow r to be in $\{3, 4\}$. Neither matroid is uniquely determined by any one of its 4-circuits.

The proofs of Theorems 1.1 and 1.2 are constructive and rely on the preliminary results in the next section. Indeed, the proof of Theorem 1.1 is essentially no more than a packaging of these results. Section 3 consists of the proofs of the two theorems. Throughout the paper, notation and terminology follows [6]. We shall also freely use the properties of spikes noted there (see, in particular, pp. 41, 73, 74, and 111) as well as the well-known fact that if C_1 and C_2 are circuits of a binary matroid, then their symmetric difference, $C_1 \triangle C_2$, is a disjoint union of circuits. For convenience, whenever we write "determined", we mean "uniquely determined".

2. Preliminaries

This section consists of five preliminary results. The first, due to Acketa [1], lists all binary paving matroids. We denote by $M(K_4^-)$ the cycle matroid of the graph obtained from K_4 by deleting an edge.

Theorem 2.1. *An n-element binary matroid is paving if and only if it is isomorphic to one of the following matroids: a loopless rank-2 matroid with*

at most three parallel classes, $U_{0,n}$, $U_{1,n}$, $U_{n,n}$, $U_{n-1,n}$, $U_{n-2,n-1} \oplus U_{1,1}$, $M(K_4^-)$, $M(K_4)$, $M(K_{3,2})$, F_7, F_7^*, *or* $AG(3,2)$.

Observe that each of the matroids $M(K_4^-)$, $M(K_4)$, F_7, F_7^*, and $AG(3,2)$ can be obtained from either a rank-3 or rank-4 binary spike by deleting at most two elements not belonging to the same leg.

Lemma 2.2. *For $r \geq 4$, let M be a matroid that is obtained from a rank-r binary spike by deleting at most $r-1$ elements no two of which belong to the same leg. Then M can be obtained from a binary spike with a cotip by adding elements in series with the cotip. Thus M is unique up to isomorphism.*

Proof. We prove the lemma when M has a tip t. The case when M has no tip is proved similarly. Let N be the rank-r binary spike with tip t and legs $\{t, x_1, y_1\}, \{t, x_2, y_2\}, \ldots, \{t, x_r, y_r\}$. By symmetry, we may assume that $M = N\backslash Z$, where $Z = \{z_1, z_2, \ldots, z_q\}$ and $z_i \in \{x_i, y_i\}$ for all i in $\{1, 2, \ldots, q\}$. Now N has $\{x_j, y_j, x_k, y_k\}$ as a cocircuit for all distinct j and k in $\{1, 2, \ldots, r\}$. Thus, for all distinct j and k in $\{1, 2, \ldots, q\}$, the set $\{x_j, y_j, x_k, y_k\} - Z$ is a disjoint union of cocircuits and hence is a cocircuit. Hence the elements of $\{x_1, y_1, x_2, y_2, \ldots, x_q, y_q\} - Z$ are in series in M. By orthogonality, it follows that the last set is a series class in M. Contracting all but one element of this series class gives a rank-$(r-q+1)$ binary spike with a tip and a cotip. Hence M is uniquely determined up to isomorphism. □

The next two lemmas deal with Theorem 1.1 when the rank-r binary matroid cannot be obtained from a binary spike by deleting at most $r-1$ elements no two of which belong to the same leg. In particular, they enable us to determine which r-element subsets of $E(M)$ are bases of M.

Lemma 2.3. *For $r \geq 3$, let M be a rank-r binary matroid, and let B be a basis of M. Suppose that M is not a restriction of a rank-r binary spike with tip. Then there is a circuit C such that $|C| \leq r-1$ and $|C - B| = 1$.*

Proof. Let $B = \{e_1, e_2, \ldots, e_r\}$, and construct a binary representation $[I_r|D]$ of M with columns labelled, in order, $e_1, e_2, \ldots, e_r, e_{r+1}, \ldots, e_n$. If there is a k in $\{r+1, r+2, \ldots, n\}$ such that the fundamental circuit $C(e_k, B)$ has size at most $r-1$, then choose C to be $C(e_k, B)$. Otherwise each of the columns in D has either $r-1$ ones or r ones. Since M is simple, it follows that M is a restriction of a rank-r binary spike with tip. □

Lemma 2.4. *For $r \geq 3$, let M be a simple rank-r binary matroid. Let B be an r-element subset of $E(M)$, and let C be a circuit of M with $|C| \leq r$ and $|C - B| = 1$. Then B is a basis of M if and only if neither B nor $B \triangle C$ contains a circuit of size at most $r-1$.*

Proof. First suppose B is a basis of M. If $B \triangle C$ contains a circuit C', then C' contains the element, f say, in $C - B$. But then, as $f \in C \cap C'$, the set $(C \cup C') - \{f\}$ contains a circuit, a contradiction as $(C \cup C') - \{f\} \subseteq B$.

Now suppose neither B nor $B \triangle C$ contains a circuit of size at most $r-1$. It suffices to show that B is not a circuit. Assume the contrary. Then $B \triangle C$ contains a circuit, which must have size r or $r+1$. But, as M is simple, $|C| \geq 3$ so $|B \triangle C| \leq r-1$; a contradiction. □

We now use the circuits of size at most $r-1$ to determine whether a simple rank-r binary matroid is a certain restriction of a rank-r binary spike.

Lemma 2.5. *For $r \geq 4$, let M be a simple rank-r binary matroid, and suppose that M is not paving. Then M can be obtained from a rank-r binary spike by deleting at most $r-1$ elements no two of which belong to the same leg if and only if, for some non-empty subset K of $\{1, 2, \ldots, r\}$, the ground set of M can be partitioned into parts $X = \{x_1, x_2, \ldots, x_r\}$, $Y = \{y_k : k \in K\}$, and Z, where $|Z| \leq 1$, such that the collection of circuits of M of size at most $r-1$ consists of*

(I) *when $|Z| = 1$, all 3-element sets of the form $\{t, x_k, y_k\}$ with $t \in Z$ and $k \in K$;*
(II) *when $r \geq 5$, all 4-element sets of the form $\{x_k, y_k, x_l, y_l\}$ with $k, l \in K$; and*
(III) *when $r \geq 6$, no sets D with $5 \leq |D| \leq r-1$.*

Proof. The proof is based on [6, Proposition 1.5.17], which identifies the set of circuits of a spike. It follows immediately from that result that if M can be obtained from a rank-r binary spike by deleting at most $r-1$ elements no two of which belong to the same leg, then $E(M)$ can be partitioned as described in the lemma. For the converse, suppose that $E(M)$ has such a partition. To show that M can be obtained from a binary spike as asserted, first note that, for distinct r-element circuits C and C' of M, since $C \triangle C'$ contains a circuit, $|C \cap C'| \leq r-2$.

We break the rest of the argument into two cases depending on whether $r \geq 5$ or $r = 4$. Suppose first that $r \geq 5$. Assume that C is not in $\big\{\{z_1, z_2, \ldots, z_r\} : \ z_i \in \{x_i, y_i\} \text{ for all } i\big\}$. Suppose $C \subseteq X \cup Y$. Then, as $|C| \geq 5$, there is a k in K with x_k, y_k in C. If $|Z| = 1$, then, as $\{t, x_k, y_k\}$ is a circuit, $C \triangle \{t, x_k, y_k\}$, which equals $(C - \{x_k, y_k\}) \cup \{t\}$, contains a circuit containing t. But $|(C - \{x_k, y_k\}) \cup \{t\}| \leq r-1$, so there are no such circuits otherwise C contains a 4-element circuit of the form in (II). Thus $Z = \emptyset$.

If $|Y| = 1$, then M is paving, so $|Y| \geq 2$. Suppose there is an l in $K - \{k\}$ such that $x_l \in C$ or $y_l \in C$. Then, as M is binary, $C \triangle \{x_k, y_k, x_l, y_l\}$

contains a circuit of size at most $r-2$. But neither $(C-\{x_k, y_k, x_l\})\cup\{y_l\}$ nor $(C-\{x_k, y_k, y_l\})\cup\{x_l\}$ contains a 3-element or a 4-element circuit of the form in (I) or (II); a contradiction. Thus, for all l in $K-\{k\}$, the set $\{x_l, y_l\}$ avoids C. Hence $|Y| = 2$ and, letting $K = \{k, l\}$, we have $C = (X-\{x_l\})\cup\{y_k\}$. Since M is binary, $C\triangle\{x_k, y_k, x_l, y_l\}$, which equals $(X-\{x_k\})\cup\{y_l\}$, contains a circuit. As no subset of this last set is of the form in (I) or (II), $(X-\{x_k\})\cup\{y_l\}$ is a circuit. It is now easily checked that M has exactly three circuits, namely, $\{x_k, y_k, x_l, y_l\}$, $(X-\{x_l\})\cup\{y_k\}$, and $(X-\{x_k\})\cup\{y_l\}$, and that M can be obtained from a rank-r tipless binary spike whose legs include $\{x_k, y_l\}$ and $\{x_l, y_k\}$ by deleting $r-2$ elements no two of which belong to the same leg.

We may now assume that $t\in C$ and so $|Z| = 1$. Let $k\in K$. Then $\{t, x_k, y_k\}$ is a circuit of M, and so, as M is binary, $C\triangle\{t, x_k, y_k\}$ contains a circuit. If either $x_k\in C$ or $y_k\in C$, then $|C\triangle\{t, x_k, y_k\}| = r-1$, and no subset of $C\triangle\{t, x_k, y_k\}$ is of the form in (I) or (II). Thus neither $x_k\in C$ nor $y_k\in C$. As $|C| = r$, we deduce that $|Y| = 1$ and $C = (X-\{x_k\})\cup\{t\}$. It is now easily checked that the circuits of M are precisely $\{t, x_k, y_k\}$, $(X-\{x_k\})\cup\{t\}$, and $X\cup\{y_k\}$, in which case, M can be obtained from a rank-r binary spike with tip y_k by deleting $r-1$ elements no two of which belong to the same leg. This competes the proof for $r\geq 5$.

Now suppose that $r = 4$. The approach is similar to that used for $r\geq 5$. Since M is not paving, it has a 3-circuit and so $|Z| = 1$. First note that, by circuit elimination, if $k, l\in K$, then $\{x_k, y_k, x_l, y_l\}$ is a 4-circuit as $\{t, x_k, y_k\}$ and $\{t, x_l, y_l\}$ are both circuits.

Let C be a 4-circuit of M that is not of the form in (II) and is not in $\big\{\{z_1, z_2, z_3, z_4\}:\ z_i\in\{x_i, y_i\}\text{ for all }i\big\}$. Suppose $t\in C$. If, for some k in K, either $x_k\in C$ or $y_k\in C$, then, as M is binary, $C\triangle\{t, x_k, y_k\}$ is a 3-circuit avoiding t; a contradiction. Thus, $|Y| = 1$ and so, letting $Y = \{k\}$, it is easily checked that $\mathcal{C}(M) = \{\{t, x_k, y_k\}, (X-\{x_k\})\cup\{t\}, X\cup\{y_k\}\}$, in which case, M can be obtained from a rank-r binary spike with tip y_k by deleting $r-1$ elements no two of which belong to the same leg.

We may now assume that $t\notin C$, and so, for some k in K, we have $\{x_k, y_k\}\subseteq C$. But then $C\triangle\{t, x_k, y_k\}$ contains a 3-circuit that is not of the form in (I); a contradiction. This completes the proof of the lemma. □

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. Since $r\geq 3$, we can determine the loops and parallel classes of M. By deleting all loops and all but one element of each parallel class, we may assume that M is simple. Moreover, we may assume that

$|E(M)| > r$ otherwise $M \cong U_{r,r}$. Suppose $r = 3$. Then M is paving. Since M is isomorphic to neither $U_{3,4}$ nor $U_{2,3} \oplus U_{1,1}$, Theorem 2.1 implies that $M \cong M(K_4^-), M(K_4)$, or F_7 . Each of these matroids can be obtained from a rank-3 binary spike by deleting at most two elements no two from the same leg. Up to isomorphism, the number of elements in M distinguishes M. Thus the theorem holds when $r = 3$.

Suppose $r \geq 4$. Assume M is paving. As M is not isomorphic to $U_{r,r+1}$ or $U_{r-1,r} \oplus U_{1,1}$, Theorem 2.1 implies that $r = 4$ and M is isomorphic to $M(K_{3,2})$, F_7^*, or $AG(3, 2)$. Each of the last two matroids can be obtained from a rank-4 binary spike by deleting at most two elements no two from the same leg. Thus, by Lemma 2.2, M is unique up to isomorphism.

We may now assume that M is not paving. By Lemma 2.5, we can determine when M can be obtained from a rank-r binary spike by deleting at most $r - 1$ elements no two of which belong to the same leg. If M can be obtained in this way, then, by Lemma 2.2, M is determined up to isomorphism. Therefore, assume that M cannot be obtained in this way. Let B be a subset of $E(M)$ with $|B| = r$. If there is no circuit C with $|C| \leq r - 1$ and $|C - B| = 1$, then, by Lemma 2.3, B is not a basis of M. But if there is such a circuit C, then, by Lemma 2.4, B is a basis of M if and only if neither B nor $B \triangle C$ contains a circuit of size at most $r - 1$. Hence we can determine if B is basis of M. Thus we can determine the collection of bases of M, thereby determining M. □

Proof of Theorem 1.2. It follows by Theorem 1.1 that we may assume M has a circuit C^+ with $|C^+| \geq r$. Let $f \in C^+$. We next determine a basis B of M with $C^+ - \{f\} \subseteq B$. If $|C^+| = r + 1$, then choose B to be $C^+ - \{f\}$. On the other hand, if $|C^+| = r$, then, by Lemma 2.4, we can find a basis of M containing $C^+ - \{f\}$, in which case, choose B to be this basis.

Let $B = \{e_1, e_2, \ldots, e_r\}$, and construct a binary representation $[I_r|D]$ of M with columns labelled, in order, $e_1, e_2, \ldots, e_r, e_{r+1}, \ldots, e_n$, where $n = |E(M)|$. We complete the proof by determining the columns of D. Let $k \in \{r+1, r+2, \ldots, n\}$. If the fundamental circuit $C(e_k, B)$ has size at most $r-1$, then the column e_k is determined. Observing that such a column has at least two ones and at most $r-2$ ones, we see that the columns e_k that are not immediately determined have either $r - 1$ ones or r ones. Since M is binary and simple, there is at most one column e_k of D with $|C(e_k, B)| = r + 1$.

Let e_l denote the column of D corresponding to f. Then e_l is determined. If $|C(e_l, B)| = r + 1$, then, for $k \neq l$, the unique zero in column e_k is in row i if and only if $\{e_i, e_k, e_l\}$ is a circuit. Since $r(M) \geq 5$, we can decide if $\{e_i, e_k, e_l\}$ is a circuit, and so we can determine e_k, and thus determine M.

Now suppose that $|C(e_l, B)| = r$. Then the column e_l has exactly one zero, say in row i. For $k \neq l$, the column e_k has no zeros if and only if $\{e_i, e_k, e_l\}$ is a circuit. Furthermore, if the column e_k has exactly one zero, then it is in row j if and only if $\{e_i, e_j, e_k, e_l\}$ is a circuit, where $i \neq j$. Since $r(M) \geq 5$, we can decide if $\{e_i, e_k, e_l\}$ and $\{e_i, e_j, e_k, e_l\}$ are circuits, and so we can determine e_k. Hence M is determined. □

Acknowledgement

The authors thank an anonymous referee for suggesting a proof of Theorem 1.1 that significantly shortened the original proof.

References

[1] D.M. Acketa, On binary paving matroids, Discrete Math. 70 (1988) 109–110.
[2] R.E. Bixby, l-matrices and a characterization of non-binary matroids, Discrete Math. 8 (1974) 139–145.
[3] C.R. Coullard, Counterexamples to conjectures on 4-connected matroids, Combinatorica 6 (1986) 315–320.
[4] J. Kahn, A problem of P. Seymour on non-binary matroids, Combinatorica 5 (1985) 319–323.
[5] J.G. Oxley, The binary matroids with no 4-wheel minor, Trans. Amer. Math. Soc. 301 (1987) 63–75.
[6] J. Oxley, Matroid Theory, Second edition, Oxford Univ. Press, New York, 2011.
[7] P.D. Seymour, On minors of non-binary matroids, Combinatorica 1 (1981) 387–394.

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana, USA

E-mail address: oxley@math.lsu.edu

School of Mathematics and Statistics, University of Canterbury, Christchurch, New Zealand

E-mail address: charles.semple@canterbury.ac.nz

School of Mathematics, Statistics and Operations Research, Victoria University of Wellington, Wellington, New Zealand

E-mail address: geoff.whittle@vuw.ac.nz