A SHORT PROOF OF NON–GF(5)–REPRESENTABILITY OF MATROIDS

JAMES GEELEN, JAMES OXLEY, DIRK VERTIGAN, AND GEOFF WHITTLE

ABSTRACT. Tutte proved that matroid is binary if and only if it does not contain a $U_{2,4}$–minor. This provides a short proof for non–$GF(2)$–representability in that we can verify that a given minor is isomorphic to $U_{2,4}$ in just a few rank evaluations. Using excluded-minor characterizations, short proofs can also be given of non–representablity over GF(3) and over GF(4). For GF(5), it is not even known whether the set of excluded minors is finite. Nevertheless, we show here that if a matroid is not representable over GF(5), then this can be verified by a short proof. Here a "short proof" is a proof whose length is bounded by some polynomial in the number of elements of the matroid. In contrast to these positive results, Seymour showed that we require exponentially many rank evaluations to prove GF(2)–representability, and this is in fact the case for any field.

1. INTRODUCTION

The main purpose of this paper is to show that if a matroid is not GF(5)–representable, then there is a short proof of this fact. To motivate the approach we first consider binary matroids. Tutte [9] proved that a matroid is binary if and only if it does not contain a minor isomorphic to $U_{2,4}$. It would require an exponential amount of work to check each 4–element minor of a matroid, so Tutte's characterization is not a practical way to show that a matroid is binary. It does however provide an extremely concise way to show that a matroid is not binary. Suppose that M is a matroid and that $N = M \setminus D/C$ is isomorphic to $U_{2,4}$. To verify that this is the case, we need to compute the rank of N and the rank of each pair of elements of N. For $X \subseteq E(N)$, $r_N(X) = r_M(X \cup C) - r_M(C)$. Therefore, we can check that N is isomorphic to $U_{2,4}$ by checking the rank of only 8 sets in M; that is, proving that a matroid is not binary requires only 8 rank evaluations.

Rota [7] conjectured that for any finite field $\mathbb{F}$ there are only finitely many minor–minimal non–$\mathbb{F}$–representable matroids. Like Tutte's characterization for binary matroids, Rota's conjecture, if true, would provide a method for proving non–$\mathbb{F}$–representability that requires only a finite number of rank evaluations. Unfortunately, Rota's conjecture is only known to be true for fields of sizes 2, 3, and 4. We consider a weaker conjecture that, for any finite field $\mathbb{F}$, there is a method for proving non–$\mathbb{F}$–representability such that the number of rank

Date: September 20, 2001.
1991 *Mathematics Subject Classification.* 05B35.

evaluations required is bounded above by a polynomial in the number of elements of the matroid.

Now consider a different approach toward characterizing binary matroids. Let M be a matroid on the ground set E and let B be a basis of M. Construct a matrix A in $\{0,1\}^{B\times(E-B)}$ such that, for $i \in B$ and $j \in E - B$, we have $A_{ij} = 1$ if and only if $(B - \{i\}) \cup \{j\}$ is a basis of M. Now, M is binary if and only if $[I, A]$ is a representation of M. Again, this does not provide a practical method for proving that M is binary since we potentially require an exponential number of rank evaluations to prove that $[I, A]$ is a representation of M. However, it only takes one rank evaluation to prove that $[I, A]$ is not a representation of M. Constructing A requires $O(|E|^2)$ rank evaluations. Hence, this method for proving that a matroid is not binary requires $O(|E|^2)$ rank evaluations.

We shall provide a method for proving non–GF(5)–representability that requires only $O(n^2)$ rank evaluations, where n denotes the number of elements of the matroid. Like the method above, our approach is to generate all possible GF(5)–representations of a matroid. This scheme hinges on the fact that 3–connected matroids have at most 6 inequivalent representations over GF(5); see [6]. Suppose that M is a non–GF(5)–representable matroid. Now, M has a non–GF(5)–representable minor that is 3–connected, so we may assume that M is 3–connected. We construct a sequence of (essentially) 3–connected matroids $M_1, \ldots, M_k$ such that M_1 is small, $M_k = M$, and M_i is a single-element extension or coextension of M_{i-1} for each $i \geq 2$. We inductively generate all representations of $M_1, \ldots, M_k$. Since M_1 is small, its representations can be generated exhaustively. Suppose that M_{i+1} is an extension of M_i. The crux of the problem is to determine the extensions of a given representation of M_i that represent M_{i+1}. The difficulty is that there are exponentially many extensions of a given representation. Using techniques from [3], we overcome this problem with a more careful choice of the sequence $M_1, \ldots, M_k$; see Corollary 3.5.

Seymour [8] showed that it is considerably harder to prove representability than non–representability. Let $\mathbb{F}$ be a field of characteristic $p > 0$. For each $r \geq \max\{4, p + 1\}$, define a matrix $[I, N_r]$ where I denotes the identity matrix whose columns are indexed by $\{a_1, \ldots, a_r\}$ and N_r is a square matrix with columns indexed by $\{b_1, \ldots, b_r\}$ that has zeros on the diagonal and ones elsewhere. Now, let M_r denote the matroid that is represented by $[I, N_r]$ over $\mathbb{F}$. Let (A, B) be a partition of $\{1, \ldots, r\}$ such that $p|(|B| - 1)$. It is an easy exercise to prove that $\{a_i : i \in A\} \cup \{b_i : i \in B\}$ is a circuit–hyperplane of M_r and that the matroid obtained by relaxing this circuit–hyperplane is not $\mathbb{F}$–representable. To distinguish M_r from each of these non–$\mathbb{F}$–representable matroids requires an exponential number of rank evaluations. Thus, to prove $\mathbb{F}$–representability we require exponentially many rank evaluations. A similar construction works for fields of characteristic zero.

2. Totally free matroids

This section contains notation and definitions and also reviews the results of [3]. Notation and terminology follow Oxley [5], with some exceptions. Here, we denote the simple and cosimple matroids canonically associated with a matroid M by $\mathrm{si}(M)$ and $\mathrm{co}(M)$, respectively.

Let M be a matroid with ground set E and let $\mathbb{F}$ be a field. Let A be a matrix over $\mathbb{F}$ whose columns are indexed by E. We denote the column–matroid of A by $M_{\mathbb{F}}(A)$. Thus A is an $\mathbb{F}$–representation of M if $M = M_{\mathbb{F}}(A)$. Let A_1 and A_2 be two matrices over $\mathbb{F}$ with columns indexed by E. We call A_1 and A_2 *strongly equivalent* if one can be obtained from the other by any sequence of the following operations:

- elementary row operations (adding one row to another, adjoining or deleting a row of zeros, and scaling a row),
- column–scaling, and
- reordering the (labelled) columns.

(This extends the definition in [2] by allowing the removal or addition of a row of zeros.) In particular, if A_1 and A_2 are strongly equivalent, then $M_{\mathbb{F}}(A_1) = M_{\mathbb{F}}(A_2)$. If $\mathbb{F}$ is a finite field with q elements, then we let $n_q(M)$ denote the number of strongly inequivalent $\mathbb{F}$–representations of M. It is well–known that $n_2(M) \leq 1$ and $n_3(M) \leq 1$ for any matroid M. However, $n_q(U_{2,4}) = q - 2 \geq 2$ for all $q \geq 4$. Moreover, if $M \oplus N$ denotes the direct sum of M and N and $M \oplus_2 N$ denotes the 2–sum of M and N, then $n_q(M \oplus N) = n_q(M)n_q(N)$ and $n_q(M \oplus_2 N) = n_q(M)n_q(N)$. Thus, when $q \geq 4$, we can obtain matroids with arbitrarily many strongly inequivalent representations. Nevertheless, by restriction our attention to 3–connected matroids, we can bound the number of representations for other small fields.

Theorem 2.1 (Kahn [4]). *If M is a 3–connected matroid, then $n_4(M) \leq 2$.*

Theorem 2.2 (Oxley, Vertigan, and Whittle [6]). *If M is a 3–connected matroid, then $n_5(M) \leq 6$.*

Our method for characterizing quinternary matroids hinges on Theorem 2.2. Unfortunately, Oxley, Vertigan and Whittle [6] showed that similar bounds cannot be obtained for any larger fields. Therefore, in order to characterize matroids representable over larger fields, we will require higher connectivity.

Let M be a matroid with ground set E. Elements $e, f \in E$ are *clones* if swapping the labels of e and f is an automorphism of M. A *clonal class* of M is a maximal set of elements of M every pair of which are clones. An element z of M is *fixed* in M if there is no single-element extension of M by an element z' in which z and z' are independent clones. Similarly, an element z of M is *cofixed* if it is fixed in M^*. Suppose that z is fixed in M, and consider two $\mathbb{F}$–representations of M of the form $[A, x]$ and $[A, x']$, where A represents $M \setminus z$. Now $[A, x, x']$ represents a single-element extension of M. Then, since z is fixed, $\{x, x'\}$ is a parallel pair. Thus $[A, x]$ and $[A, x']$ are strongly equivalent. This shows that, up to strong equivalence, any representation of $M \setminus z$ extends to at most one representation of M. This proves the following result.

Proposition 2.3. *Let z be a fixed element in a matroid M. Then $n_q(M) \leq n_q(M \setminus z)$ for any prime power q.*

Then, in order to obtain a bound on the number of strongly inequivalent representations, we can delete fixed elements and contract cofixed elements. Unfortunately, deletion and contraction may increase the number of strongly inequivalent representations. To avoid such problems, we try to maintain 3–connectivity in such deletions and contractions. Suppose that M is 3–connected. If we find a fixed element z such that $M \setminus z$ (or $\mathrm{co}(M \setminus z)$) is 3–connected, then we delete it. Similarly, if we find an element z such that $\mathrm{si}(M/z)$ is 3–connected, then we contract it. After a sequence of such deletions and contractions, we obtain a "totally free" minor. Formally, a matroid M is *totally free* if M is 3–connected and, for any element z,

(1) if z is fixed, then $\mathrm{co}(M \setminus z)$ is not 3–connected, and
(2) if z is cofixed, then $\mathrm{si}(M/z)$ is not 3–connected.

We remark that, in [3], we also required that a totally free matroid should have at least four elements. By checking the 3–connected matroids with at most three elements, it is straightforward to see that the only new matroid admitted by omitting this condition is the trivial matroid $U_{0,0}$. As a simple consequence of these definitions, we obtain the following result.

Proposition 2.4. *If M is a 3–connected matroid, then M contains a totally free minor N such that $n_q(M) \leq n_q(N)$ for any prime power q.*

The main result of [3, Theorem 2.2] is that totally free matroids do not occur sporadically, and can be found using an inductive search.

Theorem 2.5. *If M is a totally free matroid with $|E(M)| \geq 5$, then either*

- *M has an element e such that $M \setminus e$ is totally free,*
- *M has an element e such that M/e is totally free,*
- *M has elements e and f such that $M \setminus e/f$ is totally free.*

More can be said in the case that there is no single element that can be removed to obtain a totally free matroid; see [3, Corollary 8.13].

Theorem 2.6. *Let M be a totally free matroid with $|E(M)| \geq 5$ such that, for each e in $E(M)$, neither $M \setminus e$ nor M/e is totally free. Then each element z has a unique clone z'. Moreover, M/z is 3–connected, z' is fixed in M/z, and $M/z \setminus z'$ is totally free.*

A flat F of M is *cyclic* if, for each $e \in F$, there is a circuit C such that $e \in C \subseteq F$. It follows easily from definitions that F is a cyclic flat of M if and only if $E(M) - F$ is a cyclic flat of M^*. The following result is also straightforward.

Proposition 2.7. *Elements e and f of a matroid M are clones if and only if e and f are contained in the same cyclic flats.*

Let $e, f \in E(M)$. We say that e is *freer* than f if every cyclic flat containing e also contains f. Thus, e and f are clones if and only if e is freer than f and f is freer than e. The *freedom* of an element e of $E(M)$ is the maximum size of an independent clonal class containing e among all extensions of M. This maximum does not exist if and only if e is a coloop of M; in that case, the freedom of e is infinity. An element is fixed if and only if it has freedom at most 1.

The notion of freedom of an element in a matroid was introduced by Duke [1] although his definition was different from that given above. We shall show next that our definition is equivalent to Duke's.

Lemma 2.8. *Let e be an element of a matroid M. Then the freedom of e in M is the maximum over all extensions N of M of the rank of the flat of N that is the intersection of all of the cyclic flats of N containing e.*

Proof. If e has infinite freedom, then the lemma is easily checked. Thus assume that e has freedom k. Let N be an extension of M in which the clonal class containing e is X and $r_N(X) = k$. Then every cyclic flat containing e contains X. Thus, the intersection of all cyclic flats of N containing e has rank at least k. Thus the freedom of e is at most the maximum specified in the lemma statement.

Now let N be an extension of M that maximizes the rank k of the flat F that is the intersection of all cyclic flats containing e. Extend N to N' by freely adding a set Z of $k-1$ elements to F. Then $Z \cup \{e\}$ is independent in N'. We assert that $Z \cup \{e\}$ is a set of clones in N'. To see this, suppose $z \in Z$. Then a cyclic flat G of N' that contains z must also contain F and hence e. Thus z is freer than e. On the other hand, if H is a cyclic flat of N' containing e, then H must meet Z. But, as the elements of Z are freely added to F, it follows that H must contain F and hence Z. Thus e is freer than every element of Z, so

$Z \cup \{e\}$ is indeed a set of clones in N''. We conclude that the freedom of e is at least the maximum specified in the lemma statement. Therefore, the lemma holds. □

The next lemma, which will be used frequently in the paper, is Theorem 6.2 of [1]. We include a proof here for completeness.

Lemma 2.9. *Let a and b be elements of a matroid M such that a is freer than b. Then the freedom of a is at least the freedom of b. Moreover, either a and b are clones or the freedom of a is greater than the freedom of b.*

Proof. Suppose that b has freedom k and that M' is an extension of M and B is a k–element independent clonal class of M' that contains b. We may assume that $E(M') = E(M) \cup B$. We may assume that $a \notin B$ since otherwise the result is clear. Construct a matroid M'' by adding k points $\{a_1, \ldots, a_k\}$ as freely as possible in the flat of M' spanned by $B \cup \{a\}$. Now let $\hat{M}$ be the restriction of M'' to $E(M) \cup \{a_1, \ldots, a_k\}$. It is straightforward to check that a is freer than each element of B in M' so a is freer than each of $\{a_1, \ldots, a_k\}$ in $\hat{M}$. However, by construction, each of $a_1, \ldots, a_i$ is freer than a in M'' and hence also in $\hat{M}$. Thus $\{a, a_1, \ldots, a_k\}$ is contained in a clonal class of $\hat{M}$. Moreover, since B is independent in M', $\{a_1, \ldots, a_k\}$ is independent in $\hat{M}$. Hence, a has freedom at least k in M. Now, suppose that a and b are not clones, and hence that there is a cyclic flat F of M that contains b but not a. Then $B \cup \{a\}$ is independent in M', and, hence, $\{a, a_1, \ldots, a_k\}$ is independent in $\hat{M}$. Hence, a has freedom at least $k+1$ in M. □

For elements e and f of a matroid M, it is straightforward to show that the freedom of f does not decrease when we delete e. Contraction has a slightly more complicated effect on freedom.

Lemma 2.10. *Let e and f be elements of a matroid M and let k be the freedom of f. Then f has freedom at least $k-1$ in M/e. Moreover, if f has freedom exactly $k-1$ in M/e, then f is freer than e in M.*

Proof. Let M' be an extension of M that has a rank–k clonal class X containing f. Now M'/e is an extension of M/e, and $X - \{e\}$ is a clonal class of M'/e. Moreover, $r_{M'/e}(X - \{e\}) \geq |X| - 1 = k - 1$. Thus f has freedom at least $k-1$. If f is not freer than e, then there is a cyclic flat F of M' that contains f but not e. But then $X \subseteq F$ and $r_{M'/e}(X) = r_{M'}(X) = k$. Thus, f has freedom k in M/e. □

The *cofreedom* of an element e of M is the freedom of e in M^*. Note that, for $e, f \in E(M)$, e is freer than f in M^* if and only if f is freer than e in M. The following lemma is a dual version of Lemma 2.10.

Lemma 2.11. *Let e and f be elements of a matroid M and let k be the cofreedom of f. Then f has cofreedom at least $k-1$ in $M \setminus e$. Moreover, if f has cofreedom exactly $k-1$ in $M \setminus e$, then e is freer than f in M.*

Theorem 2.6 and Lemma 2.10 combine to prove the following result.

Corollary 2.12. *Let M be a totally free matroid with $|E(M)| \geq 5$ such that, for each e in $E(M)$, neither $M \setminus e$ nor M/e is totally free. Then $E(M)$ can be partitioned into 2–element clonal classes and every element of M has freedom 2.*

For representable matroids the following lemma is intuitively obvious. If two clones are "fixed to a line" and we add a new point in a way that distinguishes the two elements, then one of these elements becomes fixed.

Lemma 2.13. *Let a, b, and e be elements of a matroid M such that a and b are clones and have freedom 2 in $M \setminus e$. If a and b are not clones in M, then either a or b is fixed in M.*

Proof. Suppose that a and b are not clones in M and that neither a nor b is fixed. By possibly swapping a and b, we may assume that there is a cyclic flat F that contains a but not b. Since a is not fixed in M, there is a single-element extension M' of M by an element a' such that $\{a, a'\}$ is an independent pair of clones. Then the closure of F in M' is $F \cup \{a'\}$. Let N' be the matroid obtained by adding a point b' freely on the line between a' and b. Then every cyclic flat of N' containing b' must also contain $\{a', b\}$. Let $N = N' \setminus \{e, a'\}$. Then b' is freer than b in N. As $F \cup \{a'\}$ is a flat of M' that does not contain b, the set $\{a, a', b\}$ is independent in M'. Therefore, as $\{a', b', b\}$ is a circuit of N', the set $\{a, b', b\}$ is independent in N. Now a has freedom 2 in $M \setminus e$, and N is an extension of $M \setminus e$, so $\{a, b', b\}$ cannot be contained in a clonal class of N. Therefore, either b or b' is not a clone of a in N.

Suppose that b is not a clone of a in N. Then there is a cyclic flat F_1 that contains exactly one of a and b. Since $N \setminus b' = M \setminus e$, it follows that a and b are clones in $N \setminus b'$ so $b' \in F_1$. As b' is freer than b in N, we deduce that $b \in F_1$. Hence $a \notin F_1$. Since F' is cyclic, b' is in the closure of $F_1 - \{b'\}$ in N and hence also in N'. However, a' is in the closure of $\{b, b'\}$ in N'. So, a' is in the closure of $F_1 - \{b'\}$ in N' and hence also in M'. This contradicts the fact that a and a' are clones in M'. Thus a and b are clones in N.

We may now assume that a and b' are not clones in N. Since b' is freer than b in N, any cyclic flat containing b' also contains b, and, since a and b are clones, these flats also contain a. Therefore, there must be some cyclic flat F_2 that contains a but not b'. Since a and b are clones, F_2 contains b. However, since b' is not in the closure of F_2 in N, a' is not in the closure of F_2 in M'. This contradicts the fact that a and a' are clones in M'. □

3. Totally free matroids over small fields

The totally free matroids representable over fields with at most five elements were determined in [3]. However, we require a slightly stronger result. Before stating the result, we need to introduce some classes of totally free matroids. We begin by looking at all small totally free matroids.

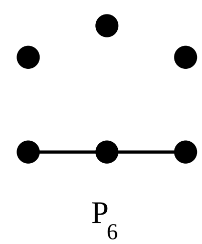

Figure 1. A 6–element totally free matroid

The two smallest totally free matroids are $U_{0,0}$ (the trivial matroid) and $U_{2,4}$. Other small totally free matroids can be found via Theorem 2.6. It is straightforward to verify the following assertions.

- $U_{2,5}$ and $U_{3,5}$ are the only 5–element totally free matroids.
- $U_{2,6}$, $U_{3,6}$, $U_{4,6}$, and P_6 are the only 6–element totally free matroids. (See Figure 1 for a geometric representation of P_6.)
- The 7–element totally free matroids are $U_{2,7}$, $U_{3,7}$, R_1, R_2, R_3, and their duals. (See Figure 2 for geometric representations of R_1, R_2, and R_3.)

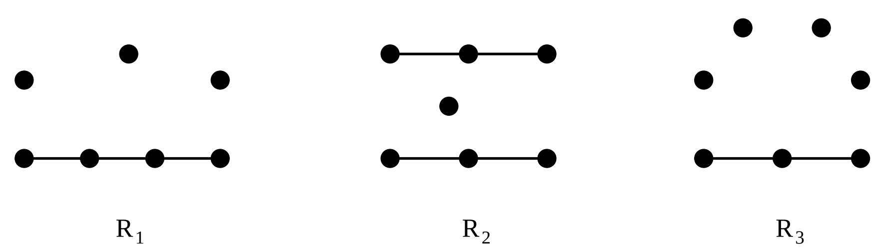

Figure 2. Some 7–element totally free matroids

Except for the trivial matroid, none of these small totally free matroids is binary and $U_{2,4}$ is the only one of these matroids that is ternary. Then, using Theorem 2.6 and Proposition 2.4, we can prove that $n_2(M) \leq 1$ and $n_3(M) \leq 1$ for any matroid M.

By results in [3], none of the 7–element totally free matroids is representable over any field with 5 or fewer elements; we include a direct proof for the sake of completeness.

Lemma 3.1. *No 7–element totally free matroid is representable over a field with 5 or fewer elements.*

Proof. Let $q \in \{2,3,4,5\}$ and let M be a 7–element totally free matroid. By duality we may assume that that M has rank at most 3. Moreover, since the 7–point line is not $GF(q)$–representable, we may assume that M has rank 3. Thus, M is either $U_{3,7}$, R_1, R_2, or R_3. In each case we suppose that M is $GF(q)$–representable and consider M as a restriction of the projective geometry $\mathrm{PG}(2,q)$.

First consider the case that $M = U_{3,7}$ and let $E(M) = \{a, b, e_1, \ldots, e_5\}$. Let L be the points of $\mathrm{PG}(2,q)$ on the line spanned by a and b. Thus, $|L - \{a,b\}| \le 4$. There are 10 distinct lines of $\mathrm{PG}(2,q)$ that are spanned by pairs of points in $\{e_1, \ldots, e_5\}$, and each of these lines contains one of the points in $L - \{a,b\}$. But then some point in $L - \{a,b\}$ is on at least 3 of these 10 lines. This is impossible, so $U_{3,7}$ is not $GF(q)$–representable. Similar arguments prove that neither R_1 nor R_2 is $GF(q)$–representable.

Now consider the case that $M = R_3$ and let $E(M) = \{a_1, a_2, a_3, e_1, e_2, e_3, e_4\}$ where $\{a_1, a_2, a_3\}$ is the unique 3–point line in R_3. Let L be the points of $\mathrm{PG}(2,q)$ on the line spanned by $\{a_1, a_2, a_3\}$ and let $L' = L - \{a_1, a_2, a_3\}$. Thus $|L'| \le 3$. Each of the 6 lines of $\mathrm{PG}(2,q)$ that is spanned by a pair of points in $\{e_1, e_2, e_3, e_4\}$ intersects the line L in a point in L'. Moreover, no point in L' can be on more than 2 of these lines. It follows that $|L'| = 3$ and that each of these points is on exactly 2 of these lines. Now, since L is a 6–point line in $\mathrm{PG}(2,q)$, it must be the case that $q = 5$. However, there are seven 3–point lines in $L' \cup \{e_1, e_2, e_3, e_4\}$, so M is isomorphic to F_7, the Fano matroid. This contradiction completes the proof. □

Let $\Lambda_3 = U_{3,6}$. For $r \ge 4$, we define a rank–r matroid Λ_r as follows. (Note that a rank–r matroid is determined by its non–spanning circuits.) We let $E(\Lambda_r) = \{a_1, \ldots, a_r\} \cup \{b_1, \ldots, b_r\}$. For any two distinct i and j in $\{1, \ldots, r\}$, the set $\{a_i, b_i, a_j, b_j\}$ is a circuit of Λ_r and these are the only non–spanning circuits. We call Λ_r the *rank–r free spike*. (In [2,3], Λ_r was denoted by Φ_r but the current notation seems more evocative.) Note that each pair $\{a_i, b_i\}$ is a clonal class of Λ_r, so Λ_r is totally free. There is a natural way to represent Λ_r over the reals: take r copunctual lines placed as freely as possible in rank r and put the elements a_i and b_i freely on the ith line. The following result is proved in [3, Theorem 2.5].

Theorem 3.2. *If M is a totally free quaternary matroid and $|E(M)| \ge 6$, then M is a free spike.*

We now define another family of totally free matroids. We let $r \ge 3$ and let $E = \{a_1, \ldots, a_r\} \cup \{b_1, \ldots, b_r\}$; the pairs $(a_1, b_1), \ldots, (a_r, b_r)$ are called the *rods*. We now describe the matroid Δ_r with ground set E by giving a representation over the reals. All subscripts are interpreted modulo r. Put points $v_1, \dots, v_r$ freely in rank r. For $i \in \{1, \dots, r\}$, we place a_i and b_i as freely as possible on the line between v_{i-1} and v_i. We call Δ_r the *rank–r free swirl.* Clearly, Δ_r is a 3–connected rank–r matroid and the elements of each rod are clones. Therefore, each free swirl is totally free. Note that $\Delta_3 = U_{3,6}$. Moreover, for $i \in \{1, \dots, r\}$, $\{a_{i-1}, a_i, b_{i-1}, b_i\}$ is a circuit and, for $r > 3$, these are the only 4–element circuits. (In [3], we denoted the free swirl by the less suggestive symbol Ψ_r.) The following result is proved in [3, Theorem 2.7].

Theorem 3.3. *If M is a totally free quinternary matroid and $|E(M)| \geq 7$, then M is a free swirl.*

The main result of this section is the following generalization of Theorems 2.1 and 2.2. We need to introduce another matroid. The Vámos matroid, V_8, is obtained from Λ_4 by relaxing one of the 4–element circuit–hyperplanes. It is well–known that V_8 is not representable over any field.

Theorem 3.4. *Let M be a totally free matroid that does not contain a minor isomorphic to any 7–element totally free matroid. If $|E(M)| \geq 8$, then either M is a free spike, M is a free swirl, or M is isomorphic to V_8.*

The following result is an easy but crucial corollary.

Corollary 3.5. *Let M be a 3–connected matroid that does not contain a minor isomorphic to any 7–element totally free matroid. If $|E(M)| \geq 7$, then M has an element e such that either e has freedom at most 2 and $co(M \setminus e)$ is 3–connected or e has cofreedom at most 2 and $si(M/e)$ is 3–connected.*

For any n we let $\mathcal{T}_n$ denote the set of all n–element totally free matroids. If a matroid M contains a minor isomorphic to some element of $\mathcal{T}_n$, we say that M contains a $\mathcal{T}_n$–minor.

Lemma 3.6. *Let M be a totally free matroid having an element e such that $M \setminus e$ is isomorphic to either Λ_4, Δ_4, or V_8. Then, M contains a $\mathcal{T}_7$–minor.*

Proof. Note that the elements of $M \setminus e$ are partitioned into 2–element clonal classes $(\{a_1, b_1\}, \dots, \{a_4, b_4\})$. Let N_i denote $M/a_i \setminus b_i$. Note that, each N_i is a single-element extension of $U_{3,6}$. Since $M \setminus e$ is 3–connected and M is totally free, e is not fixed. Thus, e is on at most one triangle of M. By possibly relabelling we may assume that e is not in a triangle with a_1 or b_1. It is now straightforward to see that N_1 is 3–connected. Thus N_1 is a 3–connected extension of $U_{3,6}$. We may assume that N_1 is not contained in $\mathcal{T}_7$. In particular, N_1 is not isomorphic to $U_{3,7}$ or R_3. Now, by considering possible extensions of $U_{3,6}$, we see that e is fixed in N_1. Then e is also fixed in M/a_1. But e is not fixed in M, so, by Lemma 2.10, e has freedom 2 in M and e is freer than a_1. By the symmetry between a_1 and b_1, e is also freer than b_1. Now, if a_1 and b_1 both have freedom 2, then, by Lemma 2.9, $\{a_1, b_1, e\}$ is an independent set of clones. However, this contradicts the fact that a_1 has freedom 2 in $M \setminus e$. We conclude that either a_1 or b_1 is fixed in M. However, $M \setminus a_1$ and $M \setminus b_1$ are both 3–connected. This contradicts the fact that M is totally free. □

Lemma 3.7. *Let M be a totally free matroid such that $M \setminus e$ is isomorphic to Λ_r or Δ_r for some $r \geq 3$. Then, M contains a $\mathcal{T}_7$–minor.*

Proof. We prove the result by induction on r. When $r = 3$, the result is trivial and, when $r = 4$, the result is implied by Lemma 3.6. Assume then that $r \geq 5$ and that the result holds for extensions of smaller free spikes and free swirls. We shall call the clonal classes $(a_1, b_1), \ldots, (a_r, b_r)$ of $M \setminus e$ *rods*. Let N_i denote $M/a_i \setminus b_i$. Note that, for any $i \in \{1, \ldots, r\}$, $N_i \setminus e$ is isomorphic to Λ_{r-1} or Δ_{r-1}. Thus, by induction, we may assume that N_i is not totally free for any i. Observe that $\Lambda_r \setminus a_i$, $\Lambda_r \setminus b_i$, $\Delta_r \setminus a_i$, and $\Delta_r \setminus b_i$ are 3–connected for each i. Therefore, $M \setminus a_i$ and $M \setminus b_i$ are 3–connected for each i. However, M is totally free, so neither a_i nor b_i is fixed. Therefore, by Lemma 2.13, a_i and b_i are clones in M and so have freedom at least 2 in M. But a_i and b_i have freedom 2 in $M \setminus e$, and therefore have freedom 2 in M.

Now M is totally free and $M \setminus e$ is 3–connected, so e is not fixed in M. By possibly relabelling the rods, we may assume that $\{a_1, b_1, e\}$ is independent. Thus, $\{a_1, b_1, e\}$ is not a set of clones of M otherwise a_1 has freedom at least 3 in $M \setminus e$; a contradiction. Thus e and a_1 are not clones in M. Therefore, by Lemma 2.9, either e is not freer than a_1, or e has freedom at least 3. In either case, by Lemma 2.10, e is not fixed in M/a_1. We deduce that e is not fixed in N_1. However, N_1 is not totally free and, for each $i > 1$, the elements a_i and b_i are clones in N_1. We conclude that e is cofixed in N_1 and $\operatorname{si}(N_1/e)$ is 3–connected. Now, e is clearly also cofixed in $M \setminus b_1$. Moreover, since e is not fixed and b_1 has freedom 2, but b_1 and e are not clones, it follows by Lemma 2.9 that b_1 is not freer than e in M. By Lemma 2.11, since e has cofreedom 1 in $M \setminus b_1$, it has cofreedom at most 2 in M. But if equality holds in the last bound, b_1 is freer than e in M. We deduce that e is cofixed in M. Now M is totally free, so $\operatorname{si}(M/e)$ is not 3–connected. Hence, there is a 2–separation (A, B) of M/e such that A and B each have rank at least 2 in M/e. Note that (A, B) is a 3–separation of $M \setminus e$, which is a free spike or a free swirl. It is straightforward to check that each rod must be contained entirely in A or entirely in B. By possibly swapping A and B, we may assume that $a_1, b_1 \in A$. Recall that $\operatorname{si}(N_1/e)$ is 3–connected, so it must be the case that $r_{N_1/e}(A - \{a_1, b_1\}) = 1$. Therefore, $r_M(A \cup e) = 3$. Thus, $A = \{a_1, b_1, a_i, b_i\}$ for some $i \in \{2, \dots, r\}$. By symmetry, we may assume that $A = \{a_1, b_1, a_2, b_2\}$.

Now, for some j in $\{3, \dots, r\}$, the set $\{a_j, b_j, e\}$ is independent. Thus, what we have proved for the rod $\{a_1, b_1\}$ also holds for $\{a_j, b_j\}$. Therefore, $|B| = 4$ and $r = 4$. This contradicts the fact that $r \geq 5$. □

We will use Theorem 2.5 to prove Theorem 3.4. Thus we must consider the matroids obtained from free spikes, free swirls, and V_8 by a single-element extension or coextension, or a single-element extension followed by a single-element coextension. Lemmas 3.6 and 3.7 consider the extension case. However, note that free spikes, free swirls, and V_8 are all self–dual. Thus, Lemmas 3.6 and 3.7 also cover the coextension case. It remains to consider the case of a single-element extension followed by a single-element coextension. Fortunately, when we are driven to this case, we obtain additional structure by Theorem 2.6.

Lemma 3.8. *If $M \in \mathcal{T}_8$ and M does not contain a $\mathcal{T}_7$–minor, then M is isomorphic to either Δ_4, Λ_4, or V_8.*

Proof. By Corollary 2.12, $E(M)$ has a unique partition into clonal classes $(\{a_1, b_1\}, \{a_2, b_2\}, \{a_3, b_3\}, \{a_4, b_4\})$ and each element of M has freedom 2. By duality we may assume that M has rank at most 4. It is straightforward to see that M must have rank 4. Moreover, the only possible non–spanning circuits of M have the form $\{a_i, b_i, a_j, b_j\}$ for $i, j \in \{1, 2, 3, 4\}$. Define a graph G with vertex set $\{1, 2, 3, 4\}$ such that $ij \in E$ if and only if $\{a_i, b_i, a_j, b_j\}$ is a circuit. Note that M is uniquely determined by G. Now, by Lemma 2.9, since a_1 is not a clone of any of a_2, a_3, and a_4, but a_1, a_2, a_3, and a_4 all have freedom 2, a_1 is not freer than any of a_2, a_3, or a_4. Thus, there are at least two distinct 4–circuits containing a_1. We conclude that each vertex of G has degree at least 2. Up to isomorphism there are now just three choices for G: a circuit, a clique, or a clique with one edge deleted. Thus, M is isomorphic to either Δ_4, Λ_4, or V_8. □

Lemma 3.9. *If $M \in \mathcal{T}_{10}$ and M does not contain a $\mathcal{T}_7$–minor, then M is isomorphic to either Δ_5 or Λ_5.*

Proof. We show first that $E(M)$ has a partition $(\{a_1, b_1\}, \dots, \{a_5, b_5\})$ into clonal classes and each element of M has freedom 2. By Corollary 2.12, this holds unless M has a $\mathcal{T}_9$–minor M_1. Consider the exceptional case. As $|E(M_1)|$ is odd, Corollary 2.12 implies that M_1 has a $\mathcal{T}_8$–minor M_2. By Lemma 3.8, since M has no $\mathcal{T}_7$–minor, M_2 is isomorphic to Δ_4, Λ_4, or V_8. Applying Lemma 3.6 to M_1 or its dual, we obtain the contradiction that M_1 has a $\mathcal{T}_7$–minor. We conclude that M has no $\mathcal{T}_9$–minor and that $E(M)$ does indeed have the specified partition into 2-element clonal classes. We call these clonal classes *rods*. Since M

has no $\mathcal{T}_9$–minor, by Theorem 2.6, M has a $\mathcal{T}_8$–minor N of rank $r(M)-1$. Since N has no $\mathcal{T}_7$–minor, Lemma 3.8 implies that $r(N)=4$. Hence $r(M)=5$. Consider a non–spanning cyclic flat F. Note that, since M is 3–connected, F is the union of 2 or 3 rods. If F is the union of 2 rods, then clearly $r_M(F)=3$.

Suppose that $F=\{a_1,b_1,a_2,b_2,a_3,b_3\}$. Let $N=M/a_5\setminus b_5$. By Theorem 2.6, N is 3–connected. Now, it follows easily that F must have rank 4 in M. We assert that F is the union of 2 cyclic flats of rank 3. Suppose otherwise. Then, by symmetry we may assume that $\{a_1,b_1,a_2,b_2\}$ and $\{a_1,b_1,a_3,b_3\}$ are both independent in M. By Theorem 2.6 and Lemma 3.8, N is isomorphic to Λ_4, Δ_4, or V_8. Thus, since $\{a_1,b_1\}$ is a clonal class of N, the sets $\{a_1,b_1,a_2,b_2\}$ and $\{a_1,b_1,a_3,b_3\}$ cannot both be independent in N. By symmetry, we assume that $\{a_1,b_1,a_2,b_2\}$ is dependent in N. Thus, $\{a_1,b_1,a_2,b_2,a_5,b_5\}$ is a cyclic flat of M. The complement of a cyclic flat of M is a cyclic flat of M^*. Thus $\{a_4,b_4,a_5,b_5\}$ and $\{a_3,b_3,a_4,b_4\}$ are cyclic flats of M^*. But then $\{a_3,b_3,a_4,b_4,a_5,b_5\}$ is a rank–4 cyclic flat of M^*, so $\{a_1,b_1,a_2,b_2\}$ is a cyclic flat of M; a contradiction. Therefore, we have proved that every rank–4 cyclic flat of M is the union of rank–3 cyclic flats.

Let $V=\{1,2,3,4,5\}$ and construct a graph G_1 with vertex set V such that $ij\in E(G_1)$ if and only if $\{a_i,b_i,a_j,b_j\}$ is a circuit. Note that M is uniquely determined by G_1. Since M is 3-connected and $r(M)=5$, each 4-circuit of M is also a flat. Define G_2 similarly with respect to M^*. Since each element of M has freedom 2 but a_1,a_2,a_3,a_4, and a_5 are in different clonal classes, it follows by Lemma 2.9 that, for each $i\geq 2$, there is a cyclic flat containing a_1 and not a_i. Thus, each vertex of G_1 and, similarly, each vertex of G_2 has degree at least two. Now, for a graph G we define a simple graph G^+ on the same vertex set as G where ij is an edge of G^+ if $G-\{i,j\}$ is connected. It is easy to check that $G_2=G_1^+$ and $G_1=G_2^+$.

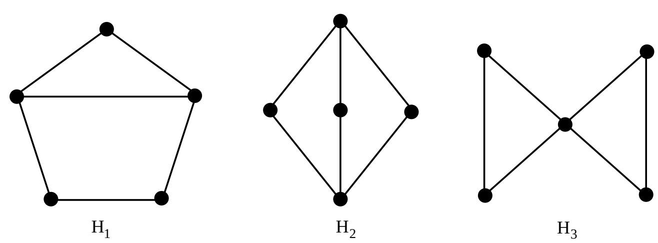

FIGURE 3. Proof of Lemma 3.9

If G_1 is either a cycle or a clique, then M is isomorphic to either Δ_5 or Λ_5. Suppose then that G_1 is not a cycle or a clique. Now suppose that G_1 contains a cycle of length 5. Since G_1 is not itself a cycle, G_1 contains the graph H_1 (see Figure 3) as a subgraph. Now,

H_1^+ is a subgraph of G_2, $(H_1^+)^+$ is a subgraph of G_1, and so forth. However, the sequence $(H_1, H_1^+, (H_1^+)^+, \ldots)$ converges to a clique so G_1 is a clique. By this contradiction we see that G_1 does not contain a cycle of length 5. Similarly, G_1 does not contain H_2 as a subgraph. Now H_3 is the only 5–vertex graph that minimum degree at least 2 and contains neither a cycle of length 5 nor H_2 as a subgraph. However, H_3^+ is not connected, so $G_1 \neq H_3$. This completes the proof. □

We are now ready to prove Theorem 3.4.

Proof of Theorem 3.4. Let M be a minor-minimal counter-example. By Theorem 2.6 and the previous lemmas, $|E(M)| \geq 12$ and $E(M)$ is partitioned into clonal classes $(\{a_1, b_1\}, \ldots, \{a_r, b_r\})$ such that $M/a_i \setminus b_i$ is isomorphic to Λ_{r-1} or Δ_{r-1} for each i in $\{1, \ldots, r\}$. We call each of these clonal classes *rods*. Obviously M has rank r and $r \geq 6$. Let $V = \{1, \ldots, r\}$ and, for $X \subseteq V$, let $R(X)$ denote $\{a_i : i \in X\} \cup \{b_i : i \in X\}$. For each k, let N_k denote $M/a_k \setminus b_k$, and let G_k denote the graph with vertex set $V - \{k\}$ and edge set E_k where $ij \in E_k$ if and only if $R(\{i, j\})$ is a circuit of N_k. Thus, G_k is either a clique or a circuit. Now let G be the graph with vertex set V and edge set E such that $ij \in E$ if and only if $R(\{i, j\})$ is a circuit of M. Note that $G - \{k\}$ is a subgraph of G_k. Moreover, if there is an edge ij of G_k that is not an edge of $G - \{k\}$, then it is straightforward to prove that $R(\{i, j, k\})$ is a cyclic flat of rank 4 in M.

Next we observe the following:

(∗) *If ij is an edge of both G_k and G_l where i, j, k, and l are distinct, then ij is an edge of G.*

To see this, note that if $ij \in E(G_k) \cap E(G_l)$, then both $R(\{i, j, k\})$ and $R(\{i, j, l\})$ are cyclic rank-4 flats of M and so $R(\{i, j\})$ is a circuit of M.

Suppose that N_1 is isomorphic to Δ_{r-1}, so G_1 is a circuit. By possibly relabelling the rods, we may assume that G_1 is the circuit $(2, 3, \ldots, r, 2)$. Note that $R(\{3, 5\}) \cup \{a_2\}$ is independent in N_1 and hence also in M. Thus, $R(\{3, 5\})$ is independent in N_2. Therefore, N_2 cannot be a spike, so N_2 is isomorphic to a free swirl. Similarly, each of $N_1, \ldots, N_r$ is isomorphic to Δ_{r-1}. Thus each of $G_1, \ldots, G_r$ is a circuit. Consider the graph G' that is the union of $G_1, \ldots, G_r$, where each edge receives a weight equal to the number of members of $\{G_1, \ldots, G_r\}$ that contain it. G is a subgraph of G'. Since each vertex i of G' has degree 2 in each G_j with $j \neq i$, the sum of the weights of the edges of G' incident with i is $2(r-1)$. Since no edge of G' has weight more than $r - 1$, it follows that at least two edges of G' have weight at least 2. By (∗), such edges are edges of G. Thus every vertex of G has degree at least two. If G has a vertex of degree at least 3 or has a circuit with fewer than $r - 1$

edges, then some $G - \{i\}$ and hence some G_i has the same property; a contradiction. We conclude that every vertex of G has degree 2 and G is a circuit. We show next that M is the free swirl Δ_r whose 4-circuits are the circuits $R(\{i,j\}$ such that $ij \in E(G)$. Specifically, we show that the non–spanning circuits of M and Δ_r coincide. The non–spanning circuits of Δ_r are all of the sets that can be formed by taking k consecutive rods for some k with $2 \le k \le r-2$ and choosing 2 elements from the first and last rods and 1 element from each of the other chosen rods. In M, the union of j consecutive rods has rank $j+1$ for all positive $j \le r-1$. Let D be a non–spanning circuit of Δ_r meeting k rods and assume that $D \cap \{a_i, b_i\}$ is empty. Then $M/a_i \backslash b_i$ has D as a circuit. Thus either D or $D \cup \{a_i\}$ is a circuit of M. In the latter case, D spans $k+1$ rods of M so $r_M(D) \ge k+2$. But D is contained in k rods of M, so $r_M(D) \le k+1$. It follows from this contradiction that every non–spanning circuit of Δ_r is a circuit of M. A similar argument shows that every non–spanning circuit of M is a circuit of Δ_r. Thus M is a free swirl.

Now consider the case that each of $N_1, \ldots, N_r$ is isomorphic to Λ_{r-1}. Then each of $G_1, G_2, \ldots, G_r$ is a clique so, by $(*)$, G is a clique. To see that M is isomorphic to Λ_r, let C be a non–spanning circuit of M that has more than 4 elements. We may assume that, for some i, the circuit C contains a_i but not b_i. Then C is a non–spanning circuit of $M/a_i \backslash b_i$. Thus $C = R(\{j,k\})$ for some j and k distinct from i. Hence $C \cup \{a_i\}$ is a circuit of M of rank 4. Now, for some l, this circuit does not span $\{a_l, b_l\}$, so it is a circuit of $M/a_l \backslash b_l$ and it is non–spanning since M has rank at least 6. As $M/a_l \backslash b_l$ is a free spike, this is a contradiction. We conclude that the only non–spanning circuits of M are the sets $R(\{i,j\})$, so M is a free spike. □

4. A short proof of non–GF(5)–representability

Let M be a matroid that is not representable over $GF(5)$. The goal is to provide a succinct proof that M is not $GF(5)$–representable. Let D and C be disjoint subsets of $E(M)$ and let $N = M \backslash D/C$. Now, for any $X \subseteq E(N)$, we have $r_N(X) = r_M(X \cup C) - r_M(C)$. Therefore, one rank evaluation for N requires only two rank evaluations for M (and if we need to make multiple rank evaluations for N, we only need to compute $r_M(C)$ once). Hence a succinct proof that N is not quinternary translates into a short proof that M is not quinternary. Thus, we may assume that each proper minor of M is $GF(5)$–representable. Moreover, we may assume that $|E(M)| \ge 8$, since otherwise we could determine M exhaustively. By Lemma 3.1, M does not contain a $\mathcal{T}_7$–minor. Now, by Corollary 3.5, there is a sequence $M_1, \ldots, M_t$ of matroids such that

- $|E(M_1)| = 6$, $M_t = M$,

- for each $i \in \{1, \ldots, t\}$, either $\mathrm{si}(M_i)$ or $\mathrm{co}(M_i)$ is 3–connected, and
- for each $i \in \{2, \ldots, t\}$, there exists $e \in E(M_i)$ such that either e has freedom at most 2 in M_i and $M_i \setminus e = M_{i-1}$ or e has cofreedom at most 2 in M_i and $M_i/e = M_{i-1}$.

Remark. Fortunately, we need not certify the aforementioned properties of the sequence $M_1, \ldots, M_t$; it suffices to know that such a sequence exists.

For each i, let $\mathcal{R}_i$ be a complete set of strongly inequivalent $GF(5)$–representations of M_i; that is, any $GF(5)$–representation of M_i is strongly equivalent to some representation in $\mathcal{R}_i$, but no two representations in $\mathcal{R}_i$ are strongly equivalent. By Theorem 2.2, $\mathcal{R}_i$ contains at most 6 representations for each i. Moreover, since M is not $GF(5)$–representable, $\mathcal{R}_t$ is empty. We will provide a succinct inductive proof that any $GF(5)$–representation of M_i is strongly equivalent to one in $\mathcal{R}_i$. Since $|E(M_1)| = 6$, the set $\mathcal{R}_1$ can be determined exhaustively.

Suppose that we have already verified that each $GF(5)$–representation of M_{k-1} is strongly equivalent to some representation in $\mathcal{R}_{k-1}$. By duality we may assume that $M_{k-1} = M_k \setminus e$ for some $e \in E(M_k)$. Let r be the rank of M_k. Consider some representation $R \in \mathcal{R}_{k-1}$. We think of R as a restriction of $\mathrm{PG}(r-1, 5)$. Let K be the set of points in $\mathrm{PG}(r-1, 5)$ that when added to R give a representation of M_k. The key point, to be proved in the theorem below, is that the rank of K is at most the freedom of e in M_k (which is at most 2).

Now, we want to generate a set of at most 6 points in $\mathrm{PG}(r-1, 5)$ that provably contains K. By considering each of the representations in $\mathcal{R}_{k-1}$, we will generate a set of at most 36 "configurations" (these are restrictions of $\mathrm{PG}(r-1, 5)$) that provably contain a representation strongly equivalent to each representation in $\mathcal{R}_k$. Any configuration that is not a representation can be rejected by a single rank computation.

It remains to generate a small set of points that provably contains K. We define this set inductively. We construct a sequence $K_0, \ldots, K_m$ of flats of $\mathrm{PG}(r-1, 5)$ as follows. Let $K_0 = PG(r-1, 5)$. For the flat K_i either:

1. There is a set $S_i \subseteq E(M_k) - \{e\}$ and an element a_i of K_i such that e is in the closure of S_i in M_k and a_i is not spanned by S_i in $\mathrm{PG}(r-1, 5)$. In this case, we define K_{i+1} to be the intersection of K_i with the flat of $\mathrm{PG}(r-1, 5)$ spanned by S_i.
2. For each flat F of M_k containing e such that e is not a coloop of $M_k|F$, the flat K_i is contained in the flat of $\mathrm{PG}(r-1, 5)$ that is spanned by $F - \{e\}$. Then $i = m$.

Note that K is contained in each of $K_0, \ldots, K_m$ and $m \leq r$. Moreover, we require only $O(r)$ rank evaluations to show that e is in the closure of each of $S_0, \ldots, S_{m-1}$ and, given

$S_0, \dots, S_{m-1}$, we can determine $K_0, \dots, K_m$ efficiently using routine linear algebra techniques. We do not need to verify the properties of K_m specified in 2; it suffices to know that such a set exists. Now we are in one of the following cases.

Case 1. There is a set $S \subseteq E(M_k) - \{e\}$ such that e is not in the closure of S in M_k but K_m is contained in the flat spanned by S in $\mathrm{PG}(r-1, 5)$.

Case 2. For each flat F of M_k that does not contain e, the flat K_m is not contained in the flat of $\mathrm{PG}(r-1, 5)$ that is spanned by F.

In Case 1, K is clearly empty. So we have a succinct proof that the representation R does not extend to a representation of M_k. Now suppose that we are in Case 2. The following theorem shows that K_m has rank at most 2. Lines in $\mathrm{PG}(r-1, 5)$ have 6 points, so there are at most 6 points in K_m. In summary, we need only $O(r)$ rank evaluations to determine $\mathcal{R}_k$ from $\mathcal{R}_{k-1}$. Therefore, we require only $O(|E|^2)$ rank evaluations to prove that M is not quinternary.

Theorem 4.1. *Let e be an element of a rank–r matroid M. Suppose that R is a $GF(q)$–representation of $M \setminus e$ considered as a restriction of $PG(r-1, q)$. Now suppose that K is a flat of $PG(r-1, q)$ such that, for each flat F of M in which e is not a coloop, $e \in F$ if and only if the flat of $PG(r-1, q)$ that is spanned by $F - \{e\}$ contains K. Then the rank of K is at most the freedom of e in M.*

Proof. Let $\mathbb{F}$ be an infinite extension field of $GF(q)$ and let $\mathcal{P}$ be the projective space of rank r over $\mathbb{F}$. Thus, $\mathcal{P}$ contains $\mathrm{PG}(r-1, q)$. Let K' be the flat of $\mathcal{P}$ that is spanned by K. Therefore, for each flat F of M in which e is not a coloop, e is in F if and only if the flat of $\mathcal{P}$ that is spanned by $F - \{e\}$ contains K'. Let K^* denote the set of points x of K' for which $R \cup \{x\}$ is an $\mathbb{F}$–representation of M. Note that an element x of K' is in K^* if and only if, for each flat F of M not containing e, the point x is not contained in the flat of $\mathcal{P}$ spanned by F. Now there is a finite number of flats F of M that do not contain e. Therefore, by a simple comparison of measures, K^* spans K'. It is now straightforward to prove that K^* is spanned by some independent set S such that S is a clonal class of the matroid M' that is represented by $R \cup S$. Note that M' is an extension of M, so $|S|$ is at most the freedom of e in M. □

Acknowledgements

Geelen was partially supported by a grant from the Natural Sciences and Engineering Research Council of Canada; Oxley and Vertigan were partially supported by grants from the National Security Agency; Whittle was partially supported by a grant from the Marsden Fund of New Zealand.

References

(1) R. Duke, Freedom in matroids, *Ars Combin.* **26B** (1988), 191–216.

(2) J. Geelen, J. Oxley, D. Vertigan, and G. Whittle, Weak maps and stabilizers of classes of matroids, *Adv. in Appl. Math.* **21** (1998), 305–341.

(3) J. Geelen, J. Oxley, D. Vertigan, and G. Whittle, Totally free expansions of matroids, *J. Combin. Theory Ser. B*, to appear.

(4) J. Kahn, On the uniqueness of matroid representations over $GF(4)$, *Bull. London Math. Soc.,* **20** (1988), 5–10.

(5) J. G. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

(6) J. Oxley, D. Vertigan, and G. Whittle, On inequivalent representations of matroids over finite fields, *J. Combin. Theory Ser. B* **67** (1996), 325–343.

(7) G.-C. Rota, Combinatorial theory, old and new. In *Proc. Internat. Cong. Math.* (Nice, Sept. 1970), pp. 229–233. Gauthier, Chichester, 1970.

(8) P. D. Seymour, Recognizing graphic matroids, *Combinatorica* **1** (1981), 75–78.

(9) W. T. Tutte, A homotopy theorem for matroids, I, II, *Trans. Amer. Math. Soc.* **88** (1958), 144–174.

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Canada

E-mail address: `jfgeelen@math.uwaterloo.ca`

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

E-mail address: `oxley@math.lsu.edu, vertigan@math.lsu.edu`

School of Mathematical and Computing Sciences, Victoria University, Wellington, New Zealand

E-mail address: `whittle@kauri.vuw.ac.nz`