JOURNAL OF COMBINATORIAL THEORY, Series B **67**, 325–343 (1996)
ARTICLE NO. 0049

On Inequivalent Representations of Matroids over Finite Fields*

James Oxley and Dirk Vertigan

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918

and

Geoff Whittle

Department of Mathematics, Victoria University, P.O. Box 600, Wellington, New Zealand

Received May 30, 1995

Kahn conjectured in 1988 that, for each prime power q, there is an integer $n(q)$ such that no 3-connected $GF(q)$-representable matroid has more than $n(q)$ inequivalent $GF(q)$-representations. At the time, this conjecture was known to be true for $q=2$ and $q=3$, and Kahn had just proved it for $q=4$. In this paper, we prove the conjecture for $q=5$, showing that 6 is a sharp value for $n(5)$. Moreover, we also show that the conjecture is false for all larger values of q.

1. INTRODUCTION

In the study of representations of matroids over finite fields, the problem of inequivalent representations arises almost immediately. For example, consider the 9-point rank-3 matroid M whose only non-trivial lines are three disjoint 3-point lines. For a large enough field F, the matroid M can be represented by a set of points in which the non-trivial lines are copunctual, and can also be represented by a set of points in which they are not; see Fig. 1. Now, automorphisms of projective planes preserve copunctuality, so it is clear that the two representations of M are inequivalent for any natural notion of equivalence of representations.

For small enough fields, this problem does not arise. It is easily seen that $GF(2)$-representations of a matroid are equivalent, and Brylawski and Lucas [4] have shown that $GF(3)$-representations are unique. Kahn [9] proved that $GF(4)$-representations are unique for 3-connected matroids.

* This paper is dedicated to Don Row who introduced all three authors to matroids.

0095-8956/96 $18.00

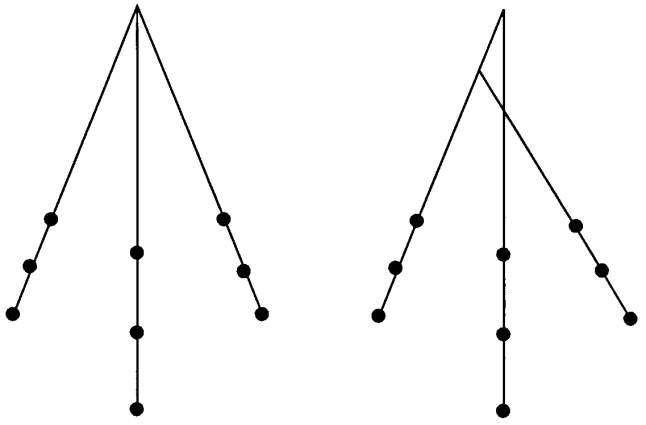

FIGURE 1

However, for $q > 4$, one cannot guarantee uniqueness of representations, even for 3-connected matroids. Given this, one could at least hope that, for such fields, the number of inequivalent representations was limited in some way. Indeed, in [9], Kahn conjectured that, for each prime power q, there is an integer $n(q)$ such that no 3-connected $GF(q)$-representable matroid has more than $n(q)$ inequivalent representations. In this paper, we prove Kahn's conjecture for $q = 5$ showing that there are at most six inequivalent $GF(5)$-representations of a 3-connected matroid. We also provide counter-examples to show that Kahn's conjecture is false for all larger values of q.

Kahn's proof that $GF(4)$-representations of 3-connected matroids are unique uses an elegant geometric argument. A crucial result needed in this argument is the following theorem of Seymour [19]. A matroid N *uses* a set X if $X \subseteq E(N)$.

(1.1) THEOREM. *If x_1 and x_2 are elements of a 3-connected nonbinary matroid M, then M has a $U_{2,4}$-minor using $\{x_1, x_2\}$.*

Our proof of Kahn's conjecture for $GF(5)$ is structured similarly to Kahn's proof for $GF(4)$. Section 3 is devoted to proving a result analogous to Theorem 1.1. The crucial fact needed is that if M is a 3-connected $GF(5)$-representable matroid with a $U_{2,4}$-restriction and a $U_{2,5}$-minor, then M has a $U_{2,5}$-minor using the elements of the $U_{2,4}$-restriction. This fact, stated as Corollary 3.10, follows immediately from more general theorems proved in Section 3. Both Theorem 1.1 and the results of Section 3 are examples of "roundedness" results. A brief discussion of such results and their role in matroid theory is included in Section 2. The proof of the conjecture for $GF(5)$, given in Section 4, then applies Corollary 3.10, using

a similar geometric argument to Kahn's proof for $GF(4)$. Not surprisingly, some complications arise which are peculiar to the $GF(5)$ case.

The counterexamples to Kahn's conjecture for $q \geqslant 7$ are given in Section 5. We present two classes of counterexamples. The first class deals with the case where the multiplicative group of $GF(5)$ has a proper subgroup of order at least three. The only cases not covered by the first class of counterexamples occur when $q = 2^k$ for some $k > 2$ such that $2^k - 1$ is prime. But, in these cases, the additive group of the field has a proper subgroup of order at least three. The second class of counterexamples includes this case.

It is of interest to ask if the results in this paper have any implications for a longstanding conjecture of Rota [14] that the set of forbidden minors for representations over $GF(q)$ is finite. This conjecture has only been proved when $q \in \{2, 3\}$ and, recently [7], when $q = 4$, and all known proofs in these cases make essential use of unique representability [1, 8, 10, 17, 21, 22]. We do not know if there is any connection between the results of this paper and the validity of Rota's conjecture in general. However, it is clear that any proof of Rota's conjecture for a prime power $q > 5$ would require significantly different techniques from those that have been used to prove the conjecture for $q \leqslant 4$.

2. PRELIMINARIES

Familiarity is assumed with the elements of matroid theory. Throughout, the terminology follows [12]. We include here a brief discussion of those aspects of matroid theory that are of particular importance for this paper.

Representations

A matroid M is *representable over a field* F or *F-representable* if there is a function φ from the ground set of M into a vector space V over F which preserves rank. In other words, $r_M(X) = r_V\{\varphi(x): x \in X\}$ for all $X \subseteq E(M)$. Equivalently, M is F-representable if and only if there is a matrix A over F whose columns are labelled by the elements of M such that, for all $X \subseteq E(M)$, the matrix consisting of the columns of A that are labelled by elements of X has rank equal to $r_M(X)$. Such a matrix is called a *representation* of M.

It is clear that a matroid is F-representable if and only if the associated simple matroid is F-representable. Thus, when considering representability questions, one frequently restricts attention to simple matroids, and we shall do this from now on. In this case, the function φ above may be viewed as a one-to-one function into a projective space over F. Indeed, it is commonplace to think of a rank-r simple F-representable matroid M as being embedded in the projective space $PG(r-1, F)$, that is, as being a

restriction of $PG(r-1, F)$. Two such embeddings φ_1 and φ_2 are *equivalent* if there is an automorphism θ of $PG(r-1, F)$ such that $\theta(\varphi_1(e)) = \varphi_2(e)$ for all e in $E(M)$. Let $|E(M)| = n$. Since there is a natural way to associate such an embedding with each $r \times n$ matrix representation of M over F, this defines equivalence of two such matrix representations. This definition can be translated into purely matrix terms as follows. First, for $r \in \{1, 2\}$, the automorphism group of $PG(r-1, F)$ is the symmetric group. Thus if $r(M) = r \leqslant 2$, then all $r \times n$ matrix representations of M over F are equivalent. If $r(M) > 2$, it follows from a theorem, sometimes known as the Fundamental Theorem of Projective Geometry, that two $r \times n$ matrix representations are equivalent if one can be obtained from the other by a sequence of the following operations. (For details, see [12, Section 6.3].)

(i) Interchange two rows.

(ii) Multiply a row by a non-zero member of F.

(iii) Replace a row by the sum of that row and another.

(iv) Interchange two columns (moving their labels with the columns).

(v) Multiply a column by a non-zero member of F.

(vi) Replace each entry of the matrix by its image under some automorphism of F.

We say that M is *uniquely representable* over F if all $r \times n$ representations of M over F are equivalent.

The fact that, by the above definition, all representations of a rank-2 matroid are equivalent has the disconcerting consequence that a matroid M and its dual may have different numbers of inequivalent representations, although this can only occur if $r(M)$ or $r(M^*)$ is 2. One could remedy this by modifying the definition so that, for representations of rank-2 matroids to be equivalent, they must be obtainable from each other via a sequence of operations (i)–(vi). Such a change does not alter the results of this paper, and we prefer to follow Kahn [9] and maintain the link between equivalence and automorphisms of the underlying projective geometry.

Roundedness

For a positive integer t, a class $\mathcal{N}$ of matroids is *t-rounded* if every member of $\mathcal{N}$ is $(t+1)$-connected and the following condition holds: If M is a $(t+1)$-connected matroid having an $\mathcal{N}$-minor and X is a subset of $E(M)$ with at most t elements, then M has an $\mathcal{N}$-minor using X. In this terminology, Seymour's theorem (1.1) amounts to saying that $\{U_{2,4}\}$ is 2-rounded.

The task of determining whether a given class of matroids is t-rounded is potentially infinite. However, Seymour [16, 20] has shown that, when t is 1 or 2, this task is finite (see also [12, Theorem 11.3.9]).

(2.1) THEOREM. *Let t be* 1 *or* 2 *and $\mathcal{N}$ be a collection of $(t+1)$-connected matroids. Then $\mathcal{N}$ is t-rounded if and only if the following condition holds: If M is a $(t+1)$-connected matroid having an $\mathcal{N}$-minor N such that $|E(M)-E(N)|=1$, and X is a subset of $E(M)$ with at most t elements, then M has an $\mathcal{N}$-minor using X.*

It is natural to extend the notion of roundedness and look, not just at the size of subsets, but at their matroid structure as well. Indeed, Reid [13] has already introduced the notion of "triangle roundedness" and his idea can be further generalized. The results in Section 3 can be interpreted in terms of such a generalization. One could say that they are results on "$U_{2,n}$-roundedness". In this light, Theorem 3.1 can be interpreted as an analogue of Theorem 2.1, and Theorem 3.2 amounts to the assertion that $\{U_{2,5}, F_7^+\}$ is "$U_{2,4}$-rounded" where F_7^+ is obtained from the Fano matroid by freely adding an element on one of the lines.

3. SOME ROUNDEDNESS RESULTS

In this section, we prove some roundedness results, one of which, Corollary 3.10, plays a crucial role in the proof of Kahn's conjecture for $q=5$.

(3.1) THEOREM. *Let M be a 3-connected matroid having a $U_{2,n+1}$-minor and a subset X such that $M \mid X \cong U_{2,n}$. Then one of the following holds.*

(a) *M has a $U_{2,n+1}$-minor using X.*

(b) *For some r in $\{3,4\}$, M has a 3-connected rank-r minor N using X such that N has a $U_{2,n+1}$-minor and $|E(N)|=2n+r-3$.*

When $n \leqslant 4$, this theorem can be strengthened. In particular, when n is 2 or 3, alternative (b) can be eliminated. This is elementary when $n=2$; for $n=3$, it follows without difficulty from Theorem 1.1. For the remainder of this section, we assume that $n \geqslant 4$. Our strengthening of Theorem 3.1 when $n=4$ involves the matroid F_7^+ that is obtained from the Fano matroid F_7 by freely adding an element on one of the lines. Clearly F_7^+ has a $U_{2,5}$-minor.

(3.2) THEOREM. *Let M be a 3-connected matroid having a $U_{2,5}$-minor and a subset X such that $M \mid X \cong U_{2,4}$. Then M has a minor N using X such that N is isomorphic to $U_{2,5}$ or F_7^+.*

Since Theorem 3.2 is a strengthening of a case of Theorem 3.1, much of the proofs of the two theorems will be common. The next four lemmas

will be used in both proofs. In each of these, M will satisfy the following condition:

(3.3) M is a 3-connected matroid having a $U_{2,n+1}$-minor and a subset X such that $M \mid X \cong U_{2,n}$. Moreover, M is a minor-minimal matroid that has these properties but has no $U_{2,n+1}$-minor using X.

Certainly if M satisfies (3.3), then $r(M) \geqslant 3$. Let the elements of X be labelled by $x_1, x_2, \ldots, x_n$.

(3.4) LEMMA. *Suppose that M satisfies* (3.3). *Then X is a modular line of M.*

Proof. The matroid M is 3-connected but has no $U_{2,n+1}$-minor using X, so X is certainly a flat of M. Hence X is a line of M. Assume that X is not modular. Then, by a well-known characterization of modular flats (see, for example, [3, Theorem 3.3] or [12, Proposition 6.9.2]), M has a hyperplane Y that avoids X. Clearly $r(X \cup Y) = r(M)$. Thus a 2-element subset $\{x_i, x_j\}$ of X can be extended to a basis for M by adding some set Z consisting of $r(M)-2$ elements of Y. Consider M/Z. This has rank 2 and contains X. If x and x' are distinct elements of X, then $r_{M/Z}(\{x, x'\}) = 2$, for otherwise $Z \cup \{x, x'\}$ has rank at most $r(M)-1$ and yet spans the basis $Z \cup \{x_i, x_j\}$ of M. Since $r_{M/Z}(Y-Z) = 1$, we may choose an element y of $Y-Z$ that is not a loop of M/Z. Then y is not parallel to an element of X in M/Z, for otherwise $Y \cap X$ contains this element. We conclude that the restriction of M/Z to $X \cup y$ is an $(n+1)$-point line; a contradiction. ∎

(3.5) LEMMA. *Suppose that M satisfies* (3.3). *If H is a hyperplane of M that does not contain X, then $|E(M) - (H \cup X)| \geqslant 2$.*

Proof. By Lemma 3.4, X is a modular line, so X must meet H. Since H does not contain X, it follows that $|X \cap H| = 1$, so $|X-H| = n-1 \geqslant 3$. If $E(M) - (H \cup X)$ is empty, then $\{H, X-H\}$ is a 2-separation of M; a contradiction. Thus we may assume that $E(M) - (H \cup X)$ contains some element e. We may also assume that e is the only such element, for otherwise the lemma holds. Therefore $r(H) + r(X-H) - r(M\backslash e) = 1$, so $\{H, X-H\}$ is a 2-separation of $M\backslash e$. Suppose this 2-separation is minimal. Then $|H| = 2$. But $|H \cap X| = 1$, so $|E(M) - X| = 2$. Thus M has a 2-element cocircuit; a contradiction. Hence the 2-separation $\{H, X-H\}$ is non-minimal. Therefore, by Bixby [2] (see also [12, Proposition 8.4.6]), M/e has no non-minimal 2-separations, and its simplification, $\widetilde{M/e}$, is 3-connected.

Now $|X \cap H| = 1$. Without loss of generality, we may assume that $X \cap H = \{x_n\}$. Since $e \notin X$, we may also assume that $X \subseteq E(\widetilde{M/e})$. Certainly $(\widetilde{M/e}) \mid X \cong U_{2,n}$. Since $\widetilde{M/e}$ is also 3-connected, the choice of M implies that $\widetilde{M/e}$ has no $U_{2,n+1}$-minor.

Let $X' = \{x_1, x_2, ..., x_{n-1}\}$. Then M has $X' \cup e$ as a cocircuit. Thus $M\backslash(X' - x_1)$ has $\{x_1, e\}$ as a cocircuit. Hence $M\backslash(X' - x_1)/x_1 \cong M\backslash(X' - x_1)/e$. Since $\widetilde{M/e}$ has no $U_{2,n+1}$-minor, $M\backslash(X' - x_1)/x_1$ has no $U_{2,n+1}$-minor. But, in M/x_1, the elements $x_2, x_3, ..., x_n$ are in parallel. Thus M/x_1 has no $U_{2,n+1}$-minor. Similarly, none of M/x_2, $M/x_3, ..., M/x_{n-1}$ has a $U_{2,n+1}$-minor. It follows that, for every $U_{2,n+1}$-minor M_1 of M, there is a subset T of X' such that M_1 uses $X' - T$, and M_1 is a minor of $M\backslash T$. Evidently, if M has a $U_{2,n+1}$-minor using at least two elements of X, then M has a $U_{2,n+1}$-minor using X. Thus $U_{2,n+1}$ is a minor of $M\backslash T$ for some $(n-2)$-element subset T of X'. But $M\backslash T$ has $(X' - T) \cup e$ as a 2-element cocircuit. Hence $M\backslash T/e$ has a $U_{2,n+1}$-minor. This contradicts the fact that $\widetilde{M/e}$ has no $U_{2,n+1}$-minor. ∎

(3.6) Lemma. *If M satisfies* (3.3), *then* $|E(M)| \geqslant r(M) + 2n - 3$.

Proof. Since M has a $U_{2,n+1}$-minor, we have $U_{2,n+1} \cong M\backslash Y/Z$ for some independent set Z and some coindependent set Y. If $|Y| \geqslant n-2$, then

$$r^*(M) \geqslant n - 2 + r^*(U_{2,n+1}) = n - 2 + n - 1,$$

and so $|E(M)| \geqslant r(M) + 2n - 3$, and the lemma holds. Thus we may assume that $|Y| \leqslant n-3$. But M has no $U_{2,n+1}$-minor using two or more elements of X, so $|X - (Y \cup Z)| \leqslant 1$. Hence $|X \cap Y| + |X \cap Z| \geqslant n-1$. Therefore, as $|X \cap Y| \leqslant n-3$, we deduce that $|X \cap Z| \geqslant 2$. It follows, since $r(X) = 2$ and Z is independent, that $|X \cap Z| = 2$. Thus $|X - Z| = n - 2$. Since every element of $X - Z$ is a loop of $M/(X \cap Z)$, we deduce that $U_{2,n+1}$ must occur as a minor of $M/(X \cap Z)\backslash(X - Z)$. Hence

$$r^*(M) \geqslant |X - Z| + r^*(U_{2,n+1}) = n - 2 + n - 1,$$

and, as before, we conclude that $|E(M)| \geqslant r(M) + 2n - 3$. ∎

(3.7) Lemma. *If M satisfies* (3.3), *then* $|E(M)| \leqslant 2n + 1$.

Proof. Lemma 2.8 of Coullard and Reid [5] describes the structure of a minor-minimal 3-connected matroid M_1 that is a minor of M using some 3-element subset X' of $E(M)$ and has a $U_{2,n+1}$-minor. If X' is a circuit $\{x_1, x_2, x_3\}$ of M, then, as in Reid [13], it is straightforward to deduce that, up to a permutation of $\{x_1, x_2, x_3\}$, one of the following occurs:

(i) $|E(M_1)| \leqslant (n+1) + 3$;

(ii) there is an element f of $E(M_1) - \{x_1, x_2, x_3\}$ such that either $\{x_1, x_2, f\}$ or $\{x_1, x_2, x_3, f\}$ is a cocircuit of M_1, and $|E(M)| = (n+1) + 4$;

(iii) there is an element f of $E(M_1)-\{x_1, x_2, x_3\}$ such that $\{x_1, x_2, f\}$ is a circuit of M_1, and $|E(M_1)| = (n+1)+4$.

As M_1 is a minor of M, we can write $M_1 = M\backslash U/V$ for some subsets U and V of $E(M)$ where V is independent and U is coindependent. Clearly $V \cap X$ is empty. Let $M_2 = M\backslash(U-X)/V$. Certainly $\widetilde{M_2}$ is 3-connected and this matroid may be labelled so that its ground set contains X. It follows from the fact that M satisfies (3.3) that $\widetilde{M_2} = M_2 = M$. Thus $(U-X)\cup V$ is empty, and so $M_1 = M\backslash(U\cap X)$ and $r(M_1) = r(M)$.

If (i) occurs, then the lemma certainly holds. If (ii) occurs, then $M_1\backslash f$, and hence $M\backslash f$, is the union of X and a hyperplane; a contradiction to Lemma 3.5. Thus we may assume that (iii) occurs. Then $f \in X$, for otherwise M has an $(n+1)$-point line using $x_1, x_2, ..., x_n$, and f. Therefore $|E(M)| = |E(M_2)| \leqslant |E(M_1)| + n - 4 = 2n+1$. ∎

Proof of Theorem 3.1. Let M be a minor-minimal matroid that satisfies the hypotheses of the theorem but has no $U_{2,n+1}$-minor using X. Then M satisfies (3.3) and so, on combining Lemmas 3.6 and 3.7, we deduce that

$$r(M) + 2n - 3 \leqslant |E(M)| \leqslant 2n+1.$$

Therefore either

(i) $r(M) = 4$ and $|E(M)| = 2n+1 = 2n+r-3$; or

(ii) $r(M) = 3$ and $|E(M)| = 2n = 2n+r-3$; or

(iii) $r(M) = 3$ and $|E(M)| = 2n+1$.

To complete the proof of Theorem 3.1, we shall show that (iii) does not occur. Assume the contrary. Since M has a $U_{2,n+1}$-minor but has no such minor using X, there is an element x of X for which M/x has a $U_{2,n+1}$-minor. In M/x, the $n-1$ elements of $X-x$ are in parallel. Thus $M/x\backslash(X-\{x, x'\})$ has a $U_{2,n+1}$-minor where $x' \in X-x$. The matroid $M/x\backslash(X-\{x, x'\})$ has exactly $n+2$ elements and rank 2. Since it has a $U_{2,n+1}$-minor, it must be isomorphic to either $U_{2,n+2}$ or the matroid that is obtained from $U_{2,n+1}$ by adding an element in parallel to one of the elements. In the latter case, let $\{y, y'\}$ be the unique 2-circuit of the matroid and, in the former case, let y be any element of the $U_{2,n+2}$-minor other than x'. In each case, $M\backslash y$ has a $U_{2,n+1}$-minor and has a $U_{2,n}$-restriction using X. Thus the choice of M implies that $M\backslash y$ is not 3-connected. But $r(M\backslash y) = 3$. Therefore every element of $M\backslash y$ lies on one of X and another line, L say. Hence M has a hyperplane, $\mathrm{cl}_M(L)$, such that $|E(M) - (X \cup \mathrm{cl}_M(L))| \leqslant 1$. This is a contradiction to Lemma 3.5. ∎

We now know that Theorem 3.1 holds. To complete the proof of Theorem 3.2, we need an additional lemma on matroids satisfying (3.3) in the special case that $n = 4$.

(3.8) LEMMA. *Suppose that* $n = 4$ *and that* M *satisfies* (3.3). *Then* $r(M) \neq 4$.

Proof. Assume that $r(M) = 4$. Then, by Lemmas 3.6 and 3.7, $|E(M)| = 9$. Let $E(M) - X = Y$. Now $M \backslash U / V \cong U_{2,5}$ for some 2-element independent set V and some 2-element coindependent set U.

Consider $M \mid Y$. As $\{Y, X\}$ is not a 2-separation of M, we deduce that $r(M \mid Y) = 4$. Moreover, if $M \mid Y$ has a coloop y, then $\mathrm{cl}_M(Y - y)$ is a hyperplane of M and $|E(M) - (X \cup \mathrm{cl}_M(Y - y))| = 1$; a contradiction to Lemma 3.5. Hence $M \mid Y \cong U_{4,5}$.

Clearly $M \backslash U / V$ contains at most one element of X. So $|(V \cup U) \cap X| \geqslant 3$. But $|U| = 2$. Therefore $|V \cap X| \geqslant 1$.

Now suppose that $|V \cap X| = 1$. Then $V \cap Y$ contains a unique element, say y. The rank-3 matroid M/y has a $U_{2,5}$-minor. Since X is a flat of M avoiding y, the matroid $\widetilde{M/y}$ may be chosen so that its ground set contains X. Therefore the choice of M implies that $\widetilde{M/y}$ is not 3-connected. But $(M/y) \mid (Y - y) \cong U_{3,4}$ so, in M/y, two of the elements of $Y - y$ must be parallel to elements of X. Hence $|\mathrm{cl}_M(X \cup y)| = 7$, so M has a 2-cocircuit; a contradiction.

We may now suppose that $|V \cap X| > 1$. Since $|V \cap X| \leqslant |V| = 2$, we conclude that $|V \cap X| = 2$. Therefore the two elements of $X - V$ are loops of M/V and so $U = X - V$. Moreover, no two elements of Y are parallel in M/V.

Now each 3-element subset of Y spans a different plane of M. Moreover, by Lemma 3.4, each of these planes meets X. Since $|Y| = 5$, there are ten such planes. But $|X| = 4$, so some point p of X lies on at least three of these planes. Choose three such planes. It is routine to show that two of these planes share two common elements of Y. The intersection of these two planes has rank at most two. Thus there is a line of M that contains p and two elements of Y. But these two elements are parallel in M/V; a contradiction. ∎

Proof of Theorem 3.2. Let M be a minor-minimal matroid satisfying the hypotheses of the theorem but having no $U_{2,5}$-minor using X. Then M satisfies (3.3) so, by Theorem 3.1 and Lemma 3.8, $r(M) = 3$ and $|E(M)| = 8$.

Now X is a modular line of M and, for some element x of X, the matroid M/x has a $U_{2,5}$-minor. But M/x has seven elements and rank 2 and has $X - x$ as a parallel class. Therefore each $U_{2,5}$-minor of M/x is obtained from it by deleting any two of the three elements of $X - x$. Thus X is the

only dependent line of M containing x. Since M is 3-connected, $M\backslash X$ is isomorphic to $U_{3,4}$ or $U_{2,3} \oplus U_{1,1}$. In the latter case, the four distinct lines of M that contain at least two elements of $E(M) - X$ must meet the line X in different points. Hence x is on two dependent lines of M; a contradiction. We conclude that $M\backslash X \cong U_{3,4}$. Moreover, every line of M that is spanned by two elements of $E(M) - X$ must meet X in some element of $X - x$. The next lemma, the straightforward proof of which is omitted, immediately implies that $M\backslash x \cong F_7$.

(3.9) LEMMA. *The only* 7*-element rank-*3 *simple matroid whose ground set can be partitioned into a* 4*-circuit and a modular line is* F_7.

Since F_7^+ is the unique simple matroid that is obtained by adding an element to one of the lines of F_7, we conclude that $M \cong F_7^+$. Hence Theorem 3.2 is proved. ▮

Since F_7 is representable only over fields of characteristic two, it follows that F_7^+ is not representable over $GF(5)$. The following corollary, which now follows immediately from Theorem 3.2, is crucial for the proof of Kahn's conjecture for $GF(5)$.

(3.10) COROLLARY. *Let* M *be a* 3*-connected* $GF(5)$*-representable matroid having a* $U_{2,5}$*-minor and a subset* X *such that* $M \mid X \cong U_{2,4}$. *Then* M *has a* $U_{2,5}$*-minor using* X.

At this stage, it is natural to ask for which fields the analogue of Corollary 3.10 holds. While this question is perhaps an aside, it has an interesting answer, for such an analogue holds only when $q \in \{2, 3, 4, 5\}$. These are exactly the values of q for which Kahn's conjecture holds. In other words, we have the following:

(3.11) PROPOSITION. *Let* q *be a prime power exceeding* 5. *Then there is a* $GF(q)$*-representable matroid* M *having a* $U_{2,q}$*-minor and a subset* X *such that* $M \mid X \cong U_{2,q-1}$ *but such that* M *has no* $U_{2,q}$*-minor using* X.

This proposition follows from examples presented at the end of Section 5. These examples are deferred to that section since they are related to the counterexamples to Kahn's conjecture for $q > 5$.

4. PROOF OF KAHN'S CONJECTURE FOR $GF(5)$

(4.1) THEOREM. *A* 3*-connected matroid has at most six inequivalent representations over* $GF(5)$.

Proof. Assume that the theorem fails and let M be a minor-minimal counterexample. Certainly M must be $GF(5)$-representable. Suppose that M is ternary. Whittle [23, Corollary 2.8] showed that a 3-connected ternary matroid has at most $q-2$ inequivalent representations over $GF(q)$ for any prime power $q>2$. It follows that M has at most three inequivalent representations over $GF(5)$. Hence we may suppose that M is non-ternary. Thus, by the excluded-minor characterization of ternary matroids [1, 17], M has $U_{2,5}$, $U_{3,5}$, F_7, or F_7^* as a minor. The last two matroids are representable only over fields of characteristic two. Thus M has $U_{2,5}$ or $U_{3,5}$ as a minor. By Oxley [11, Theorem 1.6] (see also [12, Proposition 11.2.16]), a 3-connected matroid with rank and corank at least three has a $U_{2,5}$-minor if and only if it has a $U_{3,5}$-minor. Thus either M has a $U_{2,5}$-minor, or M has a $U_{3,5}$-minor and $r^*(M)=2$. In the latter case, since M is 3-connected, $M \cong U_{n,n+2}$ for some $n \geqslant 3$. In that case, since M is $GF(5)$-representable, n is 3 or 4. We conclude that either M has a $U_{2,5}$-minor, or M is isomorphic to $U_{3,5}$ or $U_{4,6}$. The following result completes the proof of the theorem in the second case.

(4.2) LEMMA. *If n is 3 or 4, then the matroid $U_{n,n+2}$ has exactly six inequivalent representations over $GF(5)$.*

Proof. Every $GF(5)$-representation for $U_{n,n+2}$ is equivalent to one of the form $[I_n \mid A]$ where the columns of A are $[1, 1, ..., 1]^T$ and $[1, a_1, a_2, ..., a_{n-1}]^T$ and $a_1, a_2, ..., a_{n-1}$ are distinct members of $\{2, 3, 4\}$. When n is 3 or 4, there are six different choices for the column $[1, a_1, a_2, ..., a_{n-1}]^T$ subject to these restrictions. It is straightforward to check that each such choice gives a representation for $U_{n,n+2}$ and that different such choices give inequivalent representations. The lemma follows immediately. ∎

We may now assume that M has a $U_{2,5}$-minor. If $r(M)=2$, then, since the automorphism group of $PG(1,5)$ is the symmetric group on six letters, all $GF(5)$-representations of M are equivalent. Hence we may assume that $r(M) \geqslant 3$. Thus, by Oxley [11, Theorem 2.1] (see also [12, Exercise 11.2.15(i)]), M is uniform, or M has a minor isomorphic to one of the matroids P_6 and Q_6 shown in Fig. 2.

If M is uniform, then, by a result of Segre [15] (see also [12, Table 1, p. 206]), $M \cong U_{3,6}$. If M is not uniform, then, by the Splitter Theorem [18] (see also [12, Chapter 11]), either M is isomorphic to P_6 or Q_6, or M has an element x such that $M\backslash x$ or M/x is 3-connected and has a P_6- or Q_6-minor. We conclude that either

(i) M is isomorphic to $U_{3,6}$, P_6, or Q_6; or

(ii) M has an element x such that $M\backslash x$ or $M^*\backslash x$ is 3-connected and has a P_6- or Q_6-minor.

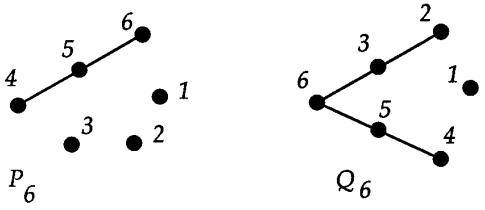

FIGURE 2

The next lemma completes the proof in case (i).

(4.3) LEMMA. *Each of the matroids $U_{3,6}$, P_6, and Q_6 has at most six inequivalent representations over GF(5).*

Proof. Let N be in $\{U_{3,6}, P_6, Q_6\}$ where $E(N) = \{1, 2, ..., 6\}$, with the labelling of P_6 and Q_6 being as in Fig. 2. Evidently $N\backslash 6 \cong U_{3,5}$. We shall now show that, for each choice of N,

(4.4) every fixed representation for $N\backslash 6$ can be extended to a representation for N in at most one way.

While proving this last assertion, we shall view a representation for $N\backslash 6$ as a restriction of $PG(2, 5)$. Clearly (4.4) holds when $N = Q_6$ for, in that case, the point 6 must lie on the intersection of the lines of $PG(2, 5)$ that are spanned by $\{2, 3\}$ and $\{4, 5\}$.

If $N = P_6$, then 6 must lie on the 6-point line of $PG(2, 5)$ that is spanned by $\{4, 5\}$. Five of the points on this line are 4, 5, and the points of intersection of L with the lines spanned by $\{1, 2\}$, $\{1, 3\}$, and $\{2, 3\}$. This leaves at most one choice for 6, so (4.4) holds when $N = Q_6$.

Now suppose that $N = U_{3,6}$. To establish (4.4) in this case, we shall assume, to the contrary, that there are two distinct points p_1 and p_2 that can be added to the fixed representation for $N\backslash 6$ to give a representation for N. By [15], $U_{3,7}$ is not $GF(5)$-representable, but $PG(2, 5) \mid \{1, 2, 3, 4, 5, p_i\} \cong U_{3,6}$ for $i = 1, 2$. Thus $PG(2, 5) \mid \{1, 2, 3, 4, 5, p_1, p_2\}$ has a unique line with more than two points. Without loss of generality, we may assume that this line is $\{p_1, p_2, 5\}$. Let L be the line of $PG(2, 5)$ containing these three points and let q_1, q_2, and q_3 be the other three points on L. Clearly if $\{i, j\}$ is a subset of $\{1, 2, 3, 4\}$, then the line of $PG(2, 5)$ spanned by $\{i, j\}$ must meet L in q_1, q_2, or q_3. It now follows by Lemma 3.9 that the restriction of $PG(2, 5)$ to $\{1, 2, 3, 4, q_1, q_2, q_3\}$ is isomorphic to F_7. This contradiction to the fact that F_7 is only representable over fields of characteristic two completes the proof that (4.4) holds for $N = U_{3,6}$, thereby finishing the proof of Lemma 4.3. ∎

We may now assume that (ii) holds. Thus M has an element x so that, for some N in $\{M, M^*\}$, the matroid $N\backslash x$ is 3-connected, has rank and corank at least three, and has a $U_{2,5}$-minor. The next lemma establishes that every representation for $N\backslash x$ extends in at most one way to a representation for N. By the choice of M, it follows from this lemma that $N\backslash x$ has at most six inequivalent $GF(5)$-representations. Hence, so does M; a contradiction. We conclude that the proof of Theorem 4.1 will be completed once we have proved the next lemma.

(4.5) LEMMA. *Let T be a spanning subset of $PG(r-1, 5)$ and suppose that $PG(r-1, 5) \mid T$ is 3-connected and has a $U_{2,5}$-minor. If y_1 and y_2 are distinct elements of $E(PG(r-1, 5)) - T$, then the map ω that fixes each element of T and takes y_1 to y_2 is not an isomorphism between $PG(r-1, 5) \mid (T \cup y_1)$ and $PG(r-1, 5) \mid (T \cup y_2)$.*

Proof. Assume, to the contrary, that ω is an isomorphism. Let L be the 6-point line of $PG(r-1, 5)$ that is spanned by $\{y_1, y_2\}$, let $X = L - \{y_1, y_2\}$, and consider $PG(r-1, 5) \mid (T \cup X)$. This matroid, M_1, is certainly 3-connected and has a $U_{2,5}$-minor. Moreover, $M_1 \mid X \cong U_{2,4}$. It now follows by Corollary 3.10 that M_1 has a $U_{2,5}$-minor using X. Let this minor be $M_1\backslash V/U$ for some independent set U and coindependent set V. Evidently $r(U) = r(M_1) - 2$. Let z be the element of $M_1\backslash V/U$ that is not in X. Then $U \cup z$ spans a hyperplane of M_1. Moreover, this hyperplane avoids X. Thus $U \cup z$ spans a hyperplane H of $PG(r-1, 5)$ that avoids X. In $PG(r-1, 5)$, the line L and the hyperplane H must meet. Since H avoids X, it contains exactly one of y_1 and y_2. Without loss of generality, we may assume that $y_1 \in H$, so $y_2 \notin H$. Thus, in $PG(r-1, 5)$, there is a circuit C containing y_1 so that $C - y_1 \subseteq U \cup z \subseteq T$. Hence C is dependent, but $\omega(C)$, which equals $(C - y_1) \cup y_2$, is not. This contradicts the assumption that ω is an isomorphism. ∎

5. THE COUNTEREXAMPLES

To show that, for all prime powers $q \geqslant 7$, the number of inequivalent $GF(q)$-representations of a 3-connected matroid M is not bounded by some constant $n(q)$, we shall consider two classes of examples. The first of these classes will establish the assertion for all prime powers q that exceed 5 and are not of the form 2^p where $2^p - 1$ is prime. Thus assume that q satisfies these conditions. The reason for imposing such conditions will be clear from the description of the example which we now give.

Consider the multiplicative group $GF(q)^*$ of non-zero elements of $GF(q)$. This group is cyclic and has $q-1$ elements. The choice of q guarantees that

$GF(q)^*$ has a proper subgroup A with at least three elements. For all $r \geqslant 3$, let M_r be the rank-r matroid that is represented by the matrix $[I_r \mid D]$ where the columns of the identity matrix are labelled by $e_1, e_2, ..., e_r$; and D is

$$\begin{array}{c} \begin{array}{cccccccccccc} f_1 & g_1 & f_2 & g_2 & f_3 & g_3 & \cdots & f_{r-1} & g_{r-1} & f_r & g_r \end{array} \\ \left[\begin{array}{cccccccccccc} 1 & 1 & 0 & 0 & 0 & 0 & & 0 & 0 & 1 & 1 \\ 1 & \alpha_1 & 1 & 1 & 0 & 0 & & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \alpha_2 & 1 & 1 & & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \alpha_3 & & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & & 1 & \alpha_{r-1} & \beta_1 & \beta_2 \end{array}\right] \end{array}$$

where each of $\alpha_1, \alpha_2, ..., \alpha_{r-1}$ is in $A - \{1\}$, and β_1, β_2 are distinct elements of $GF(q)^*$ that are not in the coset $(-1)^r A$ of the subgroup A. It will follow from the next result that M_r can be obtained from the rank-r whirl $\mathscr{W}^r$ by freely adding a point on each dependent line, and hence M_r is certainly 3-connected.

(5.1) LEMMA. *The matroid M_r does not depend on the particular choice of the $(r+1)$-tuple $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$.*

Proof. It suffices to show that the non-spanning circuits of M_r do not depend on the choice of $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$. For all i in $\{1, 2, ..., r\}$, let $C_i^* = \{f_{i-1}, g_{i-1}, e_i, f_i, g_i\}$ where all subscripts are interpreted modulo r. Evidently C_i^* is a cocircuit of M_r. Moreover, for all $j \notin \{i-1, i, i+1\}$, the matroid $M_r \backslash C_i^* / e_j$ is disconnected although $M_r \backslash C_i^*$ is connected. It is straightforward to show using this that $M_r \backslash C_i^*$ can be constructed as follows where, as before, all subscripts are read modulo r. Begin with a 4-point line on $\{e_{i+1}, f_{i+1}, g_{i+1}, e_{i+2}\}$. Take the parallel connection of this matroid with a 4-point line on $\{e_{i+2}, f_{i+2}, g_{i+2}, e_{i+3}\}$ using e_{i+2} as the basepoint. Then take the parallel connection of the resulting matroid with a 4-point line on $\{e_{i+3}, f_{i+3}, g_{i+3}, e_{i+4}\}$, this time using e_{i+3} as the basepoint. Continue in this way and conclude by taking the parallel connection of $\{e_{i-2}, f_{i-2}, g_{i-2}, e_{i-1}\}$ with the previously constructed matroid using e_{i-2} as the basepoint.

Since, for all i, the matroid $M_r \backslash C_i^*$ has the structure just described, this matroid does not depend on $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$. Thus the only non-spanning circuits of M_r that could depend on this $(r+1)$-tuple are those that meet C_i^* for all i. Let C be such a circuit. Certainly $|C| \leqslant r$. Moreover, as C meets C_i^* for all i, it follows that $|C \cap C_i^*| \geqslant 2$ for all i. Thus there are

at least $2r$ pairs (x, C_i^*) such that $x \in C \cap C_i^*$ and $1 \leqslant i \leqslant r$. Since no element of M_r is in more than two of the cocircuits $C_1^*, C_2^*, ..., C_r^*$ and $|C| \leqslant r$, it follows that there are at most $2r$ such pairs. Hence there are exactly $2r$ such pairs, $|C| = r$, and each element of C is in exactly two of the sets $C_1^*, C_2^*, ..., C_r^*$. Thus $C \subseteq \{f_1, g_1, f_2, g_2, ..., f_r, g_r\}$. Moreover, if C contains $\{f_i, g_i\}$ for some i, then C must avoid $\{f_{i+1}, g_{i+1}\}$; so C must also contain $\{f_{i+2}, g_{i+2}\}$ and avoid $\{f_{i+3}, g_{i+3}\}$, and so on. It then follows that C spans $\{e_1, e_2, ..., e_r\}$; a contradiction. We conclude that C contains exactly one element of $\{f_j, g_j\}$ for all j in $\{1, 2, ..., r\}$. Therefore the matrix whose columns are the elements of C is

$$\begin{bmatrix} 1 & 0 & 0 & & 0 & 1 \\ \gamma_1 & 1 & 0 & & 0 & 0 \\ 0 & \gamma_2 & 1 & & 0 & 0 \\ 0 & 0 & \gamma_3 & & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 0 & & \gamma_{r-1} & \beta_i \end{bmatrix}$$

where $\gamma_j \in \{1, \alpha_j\}$ for all j in $\{1, 2, ..., r-1\}$, and $i \in \{1, 2\}$. Expanding down the last column, we see that this matrix has determinant equal to $(-1)^{r-1} \gamma_1 \gamma_2 \cdots \gamma_{r-1} + \beta_i$. But this determinant is zero, and therefore $\beta_i = (-1)^r \gamma_1 \gamma_2 \cdots \gamma_{r-1}$. This is a contradiction, for $\gamma_1 \gamma_2 \cdots \gamma_{r-1}$ is certainly in the subgroup A, but β_i was chosen not to lie in the coset $(-1)^r A$. We conclude that no circuit of M_r depends on $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$. ▮

(5.2) PROPOSITION. *The matroid M_r has at least 2^r inequivalent representations over $GF(q)$.*

Proof. In the matrix $[I_r \mid D]$ representing M_r, the first non-zero entry of each row and column of D is a one. It follows without difficulty that the only way two different choices of $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$ can give equivalent representations for M_r is if the elements of one $(r+1)$-tuple can be obtained from the elements of the other by applying a fixed automorphism of $GF(q)$. Now $GF(q)$ has at most $\log_2 q$ automorphisms, so the number of inequivalent representations for M_r is at least $(\log_2 q)^{-1}$ times the number of choices for $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$. The result now follows easily since each of $\alpha_1, \alpha_2, ..., \alpha_{r-1}$ can be chosen in at least two ways, and (β_1, β_2) can be chosen in at least $((q-1)/2)((q-1)/2-1)$ ways. ▮

The above construction for N_r makes no mention of Dowling group geometries [6]. Nonetheless the example was originally discovered using these matroids. For readers familiar with Dowling geometries, the following

comments may add insight. The fact that A is a subgroup of the multiplicative group of $GF(q)$ means that $Q_r(A)$, the rank-r Dowling geometry over A, is representable over $GF(q)$. Indeed, all the elements of M_r except f_r and g_r lie in the natural $GF(q)$-representation for $Q_r(A)$. The choice of f_r and g_r outside of this representation guarantees that no unwanted dependencies arise in M_r.

To complete the proof that, for all $q \geqslant 7$, the number of inequivalent $GF(q)$-representations of a 3-connected matroid is not bounded by some constant $n(q)$, we need to look at a second class of examples to treat the case when $q = 2^t$ where $t \geqslant 3$ and $q-1$ is prime. The example will not need all these restrictions on q. Thus assume that $q = p^k$ for some prime p and some $k \geqslant 2$ where, if $p = 2$, then $k \geqslant 3$.

Let A be a proper additive subgroup of $GF(q)$ having at least three elements. For all $r \geqslant 4$, let N_r be the rank-r matroid that is represented over $GF(q)$ by the matrix $[I_r \mid D]$ where the columns of the identity matrix are labelled by $e_1, e_2, ..., e_{r-1}, g$; and D is

$$\begin{array}{c} \begin{array}{ccccccc} f_1 & f_2 & f_3 & \cdots & f_{r-1} & e_r & f_r \end{array} \\ \left[\begin{array}{ccccccc} 1 & 0 & 0 & & 0 & 1 & 1 \\ 0 & 1 & 0 & & 0 & 1 & 1 \\ 0 & 0 & 1 & & 0 & 1 & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & & \alpha_{r-1} & \beta_1 & \beta_2 \end{array}\right] \end{array}$$

where $\alpha_1, \alpha_2, ..., \alpha_{r-1}$ are non-zero elements of A, and β_1 and β_2 are distinct elements of $GF(q) - A$.

It is interesting to note that the matroid N_r depends on the additive structure of the field $GF(q)$, whereas M_r depended on the multiplicative structure of the field. In spite of this difference, the proof of the next lemma is quite similar to the proof of Lemma 5.1.

(5.3) LEMMA. *The non-spanning circuits of N_r are the sets $\{g, e_k, f_k\}$ with k in $\{1, 2, ..., r\}$, and the sets $\{e_i, e_j, f_i, f_j\}$ such that i and j are distinct elements of $\{1, 2, ..., r\}$. Hence N_r does not depend on the particular choice of $(\alpha_1, \alpha_2, ..., \alpha_{r-1}, \beta_1, \beta_2)$.*

Proof. The matroid N_r/g can be obtained from an r-element circuit on $\{e_1, e_2, ..., e_r\}$ by adding f_k in parallel with e_k for all k. Thus, for all 2-element subsets $\{s, t\}$ of $\{1, 2, ..., r\}$, the set $\{e_s, e_t, f_s, f_t\}$ is a cocircuit of N_r/g and hence of N_r. Moreover, $N_r/g \backslash \{e_s, e_t, f_s, f_t\}$ is the direct sum of $r-2$ two-element circuits. It follows easily that $N_r \backslash \{e_s, e_t, f_s, f_t\}$ is

obtained by taking the parallel connection of the $r-2$ three-point lines $\{g, e_k, f_k\}$ for which $k \in \{1, 2, ..., r\} - \{s, t\}$. Hence, as $r \geqslant 4$, each of the sets specified in the statement of the lemma is a non-spanning circuit of N_r. Suppose that N_r has some other non-spanning circuit C. Then C must meet all of the sets $\{e_s, e_t, f_s, f_t\}$ where s and t are distinct elements of $\{1, 2, ..., r\}$. Therefore, as each of these sets $\{e_s, e_t, f_s, f_t\}$ is a cocircuit of N_r and $|C| \leqslant r$, it follows that $C = \{d_1, d_2, ..., d_r\}$ where $d_k \in \{e_k, f_k\}$ for all k. Thus $C - \{e_1, e_2, ..., e_{r-1}\}$ is a circuit of $N_r/(C \cap \{e_1, e_2, ..., e_{r-1}\})$. Hence, for some subset $\{k_1, k_2, ..., k_m\}$ of $\{1, 2, ..., r-1\}$ and some i in $\{1, 2\}$, the matrix

$$\begin{bmatrix} 1 & 0 & & 0 & 1 \\ 0 & 1 & & 0 & 1 \\ 0 & 0 & & 0 & 1 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & & 1 & 1 \\ \alpha_{k_1} & \alpha_{k_2} & & \alpha_{k_m} & \beta_i \end{bmatrix}$$

has zero determinant. Thus the columns of this matrix are linearly dependent. It follows easily that $\alpha_{k_1} + \alpha_{k_2} + \cdots + \alpha_{k_m} = -\beta_i$. But the element on the left-hand side of this equation is in A, whereas $-\beta_i$ is certainly not. This contradiction completes the proof that the only non-spanning circuits of N_r are as specified in the lemma. ∎

It follows without difficulty from the last lemma that the matroid N_r is 3-connected.

(5.4) PROPOSITION. *The matroid N_r has at least 2^{r-1} inequivalent representations over $GF(q)$.*

Proof. In the matrix $[I_r \mid D]$ representing N_r, multiply the last row of D by α_1^{-1} to get D'. The matrix $[I_r \mid D']$ still represents N_r and this matrix has the maximum number of entries that, by row and column scaling, can be predetermined to equal one (see, for example, [12, Section 6.4]). Now argue as in the proof of Proposition 5.2. Each of $\alpha_2, \alpha_3, ..., \alpha_{r-1}$ can be chosen in at least two ways since $|A| \geqslant 3$. Moreover, (β_1, β_2) can be chosen in at least $(q/2)(q/2-1)$ ways. Thus the number of inequivalent representations for N_r is at least $2^{r-2}p^{k-1}(p^{k-1}-1)\,k^{-1}$ since $\log_p q = k$. The proposition now follows easily. ∎

We now consider the examples which establish Proposition 3.11. For the first example, we assume that q is an odd prime power exceeding 5. Since $GF(q)^*$ is cyclic of even order, it has a subgroup A of order $(q-1)/2$.

Define sets of vectors over $GF(q)$ as follows: $S_1 = \{[1, \alpha, 0]^T : \alpha \in A\}$; $S_2 = \{[1, 0, -\alpha]^T : \alpha \in A\}$; $S_3 = \{[0, 1, 0]^T, [0, 0, 1]^T\} \cup \{[0, 1, \alpha]^T : \alpha \in A\}$; and, finally, S_4 consists of all but two of the points of the form $[0, 1, x]^T$ that are not in S_3. The fact that $q \geqslant 7$ guarantees that S_4 is non-empty. Let M_A be the matroid represented over $GF(q)$ by $S_1 \cup S_2 \cup S_3 \cup S_4$. Evidently, $M_1 \mid (S_3 \cup S_4) \cong U_{2, q-1}$. Moreover, it is straightforward to verify that M_A has a $U_{2, q}$-minor, and that M_A has no $U_{2, q}$-minor using $S_3 \cup S_4$.

For readers familiar with Dowling geometries, the above verifications are particularly easy. The sets S_1, S_2, and S_3 have been chosen so that $\{[1, 0, 0]^T\} \cup S_1 \cup S_2 \cup S_3$ is a representation over $GF(q)$ of the rank-3 Dowling geometry over A. This guarantees that, for $\mathbf{a} \in S_1$ and $\mathbf{b} \in S_2$, the line $\mathrm{cl}_{M_A}\{\mathbf{a}, \mathbf{b}\}$ meets the line $S_3 \cup S_4$, and does so in an element of S_3. It follows that the only non-trivial line passing through an arbitrary point $\mathbf{p}$ of S_4 is the line $S_3 \cup S_4$, and therefore $\widetilde{M_A/\mathbf{p}} \cong U_{2, q}$. It also follows that if $\mathbf{x} \in S_1 \cup S_2$, then $\widetilde{M_A/\mathbf{x}} \cong U_{2, q-1}$. We conclude that M_A has no $U_{2, q}$-minor using $S_3 \cup S_4$.

Now assume that $q = 2^k$, where $k > 2$. Then the additive group of $GF(q)$ has even order, and, since this group is abelian, it has a subgroup A of order $q/2$. In this case, define sets of vectors over $GF(q)$ as follows: $S_1 = \{[1, 0, \alpha]^T : \alpha \in A\}$; $S_2 = \{[0, 1, \alpha]^T : \alpha \in A\}$; $S_3 = \{[1, 1, \alpha]^T : \alpha \in A\} \cup \{[0, 0, 1]^T\}$; and S_4 consists of all but two points of the set $\{[1, 1, \beta]^T : \beta \notin A\}$. The fact that $q \geqslant 8$ guarantees that S_4 is non-empty. Let N_A be the matroid represented over $GF(q)$ by $S_1 \cup S_2 \cup S_3 \cup S_4$. Clearly $N_A \mid (S_3 \cup S_4) \cong U_{2, q-1}$. It is routine to verify that, for $\mathbf{a} \in S_1$ and $\mathbf{b} \in S_2$, the line $\mathrm{cl}_{N_A}\{\mathbf{a}, \mathbf{b}\}$ meets the line $S_3 \cup S_4$, and does so in an element of S_3. It follows from this that if $\mathbf{p} \in S_4$, then $\widetilde{N_A/\mathbf{p}} \cong U_{2, q+1}$, so N_A certainly has a $U_{2, q}$-minor. It also follows that if $\mathbf{x} \in S_1 \cup S_2$, then $\widetilde{N_A/\mathbf{x}} \cong U_{2, q-1}$. We conclude that N_A has no $U_{2, q}$-minor using $S_3 \cup S_4$.

Finally, it is worth noting that, just as with the matroids M_r and N_r defined before, the matroids M_A and N_A are constructed using properties of the multiplicative and additive groups of the field, respectively.

ACKNOWLEDGMENT

This research was partially supported by a grant from the Louisiana Education Quality Support Fund through the Board of Regents and by a grant from the National Security Agency.

REFERENCES

1. R. E. Bixby, On Reid's characterization of the ternary matroids, *J. Combin. Theory Ser. B* **26** (1979), 174–204.
2. R. E. Bixby, A simple theorem on 3-connectivity, *Linear Algebra Appl.* **45** (1982), 123–126.

3. T. H. Brylawski, Modular constructions for combinatorial geometries, *Trans. Amer. Math. Soc.* **203** (1975), 1–44.
4. T. H. Brylawski and D. Lucas, Uniquely representable combinatorial geometries, *in* "Teorie Combinatorie, Proc. 1973 Internat. Colloq.," pp. 83–104, Accademia Nazionale dei Lincei, Rome, 1976.
5. C. R. Coullard and T. J. Reid, Element subsets of 3-connected matroids, *Congress. Numer.* **66** (1988), 81–92.
6. T. A. Dowling, A class of geometric lattices based on finite groups, *J. Combin. Theory Ser. B* **14** (1973), 61–86; erratum, **15** (1973), 211.
7. J. Geelen, A. M. H. Gerards, and A. Kapoor, in preparation.
8. J. Kahn, A geometric approach to forbidden minors for $GF(3)$, *J. Combin. Theory Ser. A* **37** (1984), 1–12.
9. J. Kahn, On the uniqueness of matroid representations over $GF(4)$, *Bull. London Math. Soc.* **20** (1988), 5–10.
10. J. Kahn and P. D. Seymour, On forbidden minors for $GF(3)$, *Proc. Amer. Math. Soc.* **102** (1988), 437–440.
11. J. G. Oxley, A characterization of certain excluded-minor classes of matroids, *Europ. J. Combin.* **10** (1989), 275–279.
12. J. G. Oxley, "Matroid Theory," Oxford Univ. Press, New York, 1992.
13. T. J. Reid, "On Roundedness in Matroid Theory," Ph.D. dissertation, Louisiana State University, 1988.
14. G.-C. Rota, Combinatorial theory, old and new, *in* "Proc. Internat. Cong. Math., Nice, 1970," pp. 229–233, Gauthier-Villars, Paris, 1971.
15. B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura. Appl.* **39** (1955), 357–379.
16. P. D. Seymour, A note on the production of matroid minors, *J. Combin. Theory Ser. B* **22** (1977), 289–295.
17. P. D. Seymour, Matroid representation over $GF(3)$, *J. Combin. Theory Ser. B* **26** (1979), 159–173.
18. P. D. Seymour, Decomposition of regular matroids, *J. Combin. Theory Ser. B* **28** (1980), 305–359.
19. P. D. Seymour, On minors of non-binary matroids, *Combinatorica* **1** (1981), 387–394.
20. P. D. Seymour, Minors of 3-connected matroids, *Europ. J. Combin.* **6** (1985), 375–382.
21. K. Truemper, Alpha-balanced graphs and matrices and $GF(3)$-representability of matroids, *J. Combin. Theory Ser. B* **32** (1982), 112–139.
22. W. T. Tutte, A homotopy theorem for matroids, I, II, *Trans. Amer. Math. Soc.* **88** (1958), 144–174.
23. G. P. Whittle, Inequivalent representations of ternary matroids, *Discrete Math.* **149** (1996), 233–238.