Journal of Combinatorial Theory, Series B 100 (2010) 740–743

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series B

www.elsevier.com/locate/jctb

On inequivalent representations of matroids over non-prime fields

Jim Geelen [a,1], Bert Gerards [b], Geoff Whittle [c]

[a] *Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Canada*
[b] *Centrum Wiskunde & Informatica, Amsterdam, The Netherlands*
[c] *School of Mathematical and Computing Sciences, Victoria University, Wellington, New Zealand*

ARTICLE INFO

Article history:
Received 2 April 2009
Available online 16 August 2010

Keywords:
Matroids
Inequivalent representations
Connectivity

ABSTRACT

For each finite field $\mathbb{F}$ of *prime* order there is a constant c such that every 4-connected matroid has at most c inequivalent representations over $\mathbb{F}$. We had hoped that this would extend to all finite fields, however, it was not to be. The (m,n)-*mace* is the matroid obtained by adding a point freely to $M(K_{m,n})$. For all $n \geqslant 3$, the $(3,n)$-mace is 4-connected and has at least 2^n representations over any field $\mathbb{F}$ of non-prime order $q \geqslant 9$. More generally, for $n \geqslant m$, the (m,n)-mace is vertically $(m+1)$-connected and has at least 2^n inequivalent representations over any finite field of non-prime order $q \geqslant m^m$.

1. Introduction

For every finite field $\mathbb{F}$ of non-prime order $\geqslant 9$, we show that there are 4-connected matroids having arbitrarily many inequivalent representations over $\mathbb{F}$. This is in striking contrast to the situation for fields of prime order. Earlier we proved that, for each finite field $\mathbb{F}$ of *prime* order, there is a constant c such that every 4-connected matroid has at most c inequivalent representations over $\mathbb{F}$; see [1]. This dichotomy came as a surprise to us. In fact, we fully expected that the proof of the result for prime fields would extend routinely to the non-prime case. When we came to write the proof our illusions had an awkward encounter with reality. After a time, and an increasingly desperate flurry of email correspondence, we were left staring glumly at the culprits.

The (m,n)-*mace* is the matroid obtained by adding a point freely to $M(K_{m,n})$, where $K_{m,n}$ is the complete bipartite graph with colour-classes of size m and n respectively. Let M be an (m,n)-mace,

[1] This research was partially supported by grants from the Natural Sciences and Engineering Research Council of Canada and the Marsden Fund of New Zealand.

0095-8956/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jctb.2010.08.001

with $m \leqslant n$. Since $M(K_{m,n})$ is vertically m-connected, M is vertically $(m+1)$-connected. Since $K_{m,n}$ has no triangles, the $(3,n)$-mace is 4-connected for each $n \geqslant 3$.

We assume that the reader is familiar with matroid representation. We mostly use the notation and definitions of Oxley [4]. In this paper, however, we say that two representations are *equivalent* if one can be obtained from the other by elementary row operations and column scaling. We do not allow the use of field automorphisms.

For a prime-power $q = p^k$ we define

$$m_q = \begin{cases} (k-1)(p-1)+1, & p \geqslant 3, \\ k-1, & p = 2. \end{cases}$$

Theorem 1.1. *Let $\mathbb{F}$ be a finite field of order $q = p^k$ where p is prime and $k \geqslant 2$. If $m \leqslant m_q$, then the (m,n)-mace has at least 2^n inequivalent representations over $\mathbb{F}$.*

The following result is an immediate corollary of Theorem 1.1.

Corollary 1.2. *For any finite field $\mathbb{F}$ of non-prime order $q \geqslant 9$ and any integer c, there is a 4-connected matroid with at least c inequivalent representations over $\mathbb{F}$.*

Corollary 1.2 leaves two exceptional fields, namely GF(4) and GF(8). Kahn [2] proved that all 3-connected matroids have at most two inequivalent representations over GF(4). We conjecture that there is an integer c such that every 4-connected matroid has at most c inequivalent representations over GF(8).

Let $\mathbb{F}_+$ be the additive group of a finite field $\mathbb{F}$. Subgroups of $\mathbb{F}_+$ play an important role in representing a mace (which is why maces do not cause difficulties for fields of prime order). The following lemma is an immediate consequence of Lemma 2.3 which is proved in the next section.

Lemma 1.3. *If Γ is a subgroup of $\mathbb{F}_+$ and there exists a sequence $(\alpha_1, \ldots, \alpha_{m-1})$ of elements in $\mathbb{F}$ such that no non-empty subsequence sums to an element of Γ, then the (m,n)-mace has at least $(|\Gamma|-1)^n$ inequivalent representations over $\mathbb{F}$.*

Suppose that $|\mathbb{F}| = p^k$ for some prime p and integer k; thus $\mathbb{F}_+ = \mathbb{Z}_p^k$. To obtain matroids with many inequivalent representations from Lemma 1.3, we require $|\Gamma| \geqslant 3$. For $p \geqslant 3$ we choose $\Gamma = \mathbb{Z}_p$ and, for $p = 2$, we choose $\Gamma = \mathbb{Z}_2^2$. We would like to know the length of the longest sequence of elements in $\mathbb{F}$ such that no non-empty subsequence sums to an element of Γ; we denote this number by $m(\Gamma) - 1$. Note that $m(\Gamma)$ is the smallest integer such that any sequence of $m(\Gamma)$ elements in the quotient group $\mathbb{F}_+/\Gamma$ has a non-empty subsequence that adds to zero; this is exactly the *Davenport constant* of the group $\mathbb{F}_+/\Gamma$. Note that $\mathbb{F}_+/\Gamma = \mathbb{Z}_p^t$ where $t = k-1$ when $p \geqslant 3$, and $t = k-2$ when $p = 2$. The Davenport constant of $\mathbb{Z}_p^t$ is known to be $t(p-1)+1$; see Olsen [3]. Therefore $m(\Gamma) = m_q$ and, hence, Theorem 1.1 is a consequence of Lemma 1.3.

Kahn [2] conjectured that for each finite field $\mathbb{F}$ there is a constant c such that every 3-connected matroid has at most c inequivalent representations over $\mathbb{F}$. Kahn's conjecture was refuted by Oxley, Vertigan, and Whittle [5] for all fields of order $\geqslant 7$. Our results show that Kahn's conjecture cannot be revived by replacing 3-connected by vertically k-connected for any fixed integer k. However we believe that maces are, in some sense, as bad as it gets.

Conjecture 1.4. *For any finite field $\mathbb{F}$ of non-prime order q there exists an integer c such that every (m_q+2)-connected matroid has at most c inequivalent representations over $\mathbb{F}$.*

2. Extensions of graphic matroids

Let $\mathbb{F}$ be a field and let $G = (V, E)$ be a graph with $V = \{1, \ldots, n\}$. Now let A be the *signed-incidence matrix* of G; that is, the rows of A are indexed by vertices, the columns are indexed by edges, and, for an edge $e = ij$, with $i < j$, the i-th entry is 1, the j-th entry is -1, and all other entries are zero. For $\alpha \in \mathbb{F}^V$, we let $M(G,\alpha)$ denote the matroid represented by $[A,\alpha]$ over $\mathbb{F}$. Thus $M(G,\alpha)$ is a single element extension of $M(G)$; we call the new element t. The following matrix shows $[A,\alpha]$ in the case that $G = K_{3,3}$.

$$\begin{array}{|ccc|ccc|ccc|c|}
\hline
e_{14} & e_{15} & e_{16} & e_{24} & e_{25} & e_{26} & e_{34} & e_{35} & e_{36} & t \\
\hline
\hline
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \alpha_2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \alpha_3 \\
\hline
-1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & \alpha_4 \\
0 & -1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & \alpha_5 \\
0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & -1 & \alpha_6 \\
\hline
\end{array}$$

For $S \subseteq V$, we let $\alpha(S) = \sum(\alpha_i\colon\ i \in S)$. The following facts are straightforward.

(i) If $M = M_{\mathbb{F}}(B)$, for some matrix B over $\mathbb{F}$, and $M \setminus t = M(G)$, then B is equivalent to $[A,\alpha]$ for some $\alpha \in \mathbb{F}^V$.
(ii) If G is 2-connected and $\alpha, \alpha' \in \mathbb{F}^V$ are non-zero vectors, then $[A,\alpha]$ and $[A,\alpha']$ are equivalent if and only if α is a scalar multiple of α'.
(iii) For $\alpha \in \mathbb{F}^V$, the element t is spanned by E in $M(G,\alpha)$ if and only if, for each component H of G, we have $\alpha(V(H)) = 0$.

The next lemma follows immediately from (iii).

Lemma 2.1. *Let $G = (V,E)$ be a connected graph and let $\alpha \in \mathbb{F}^V$ with $\alpha(V) = 0$. Then t is freely placed in $M(G,\alpha)$ if and only if there is no subgraph F of G such that F is not connected, and $\alpha(V(H)) = 0$ for each component H of F.*

We let the bipartition in $K_{m,n}$ be $(\{1,\dots,m\},\{m+1,\dots,m+n\})$. The following result is a specialization of Lemma 2.1 to extensions of $M(K_{m,n})$.

Lemma 2.2. *Let $\alpha \in \mathbb{F}^{m+n}$ with $\alpha(\{1,\dots,m+n\}) = 0$. Then $M(K_{m,n},\alpha)$ is the (m,n)-mace if and only if $\alpha_i \neq 0$ for each $i \in \{1,\dots,m+n\}$, and $\alpha(S) \neq 0$ for each $S \subseteq \{1,\dots,m+n\}$ with $1 \leqslant |S \cap \{1,\dots,m\}| < m$ and $1 \leqslant |S \cap \{m+1,\dots,m+n\}| < n$.*

Lemma 2.3. *Let Γ be a subgroup of $\mathbb{F}_+$. Let $\alpha_1,\dots,\alpha_{m-1}$ be a sequence of elements in $\mathbb{F}$ such that no non-empty subsequence adds to an element of Γ, let $\alpha_{m+1},\dots,\alpha_{m+n} \in \Gamma - \{0\}$, and define α_m so that $\alpha(\{1,\dots,m+n\}) = 0$. Then $M(K_{m,n},\alpha)$ is the (m,n)-mace.*

Proof. Certainly $\alpha_1,\dots,\alpha_{m+n}$ are all non-zero. Suppose that there exists $S \subseteq \{1,\dots,m+n\}$ such that $1 \leqslant |S \cap \{1,\dots,m\}| < m$, $1 \leqslant |S \cap \{m+1,\dots,m+n\}| < n$, and $\alpha(S) = 0$. By possibly replacing S with $\{1,\dots,m+n\} - S$ we may assume that $m \notin S$. Since $\alpha(S) = 0$, we have $\alpha(S \cap \{1,\dots,m-1\}) = -\alpha(S \cap \{m+1,\dots,m+n\}) \in \Gamma$. This gives a non-empty subsequence of $(\alpha_1,\dots,\alpha_{m-1})$ that sums to an element of Γ. This contradiction completes the proof. □

3. A more general construction

For $n \geqslant m > 3$, the (m,n)-mace is vertically $(m+1)$-connected but is not even 5-connected. In this section we briefly sketch a proof of the following theorem.

Theorem 3.1. *Let $\mathbb{F}$ be a finite field of non-prime order q. For any positive integer c, there is an (m_q+1)-connected matroid that has at least c inequivalent representations over $\mathbb{F}$.*

The result holds for $q = 4$ (consider 2-sums of copies of $U_{2,4}$), so we may assume that $q \neq 4$. Let $m = m_q$, $g = m_q + 1$, and $n = \lceil \log_2 c \rceil$. There exists an m-regular, internally $(m+1)$-connected graph H with girth at least g. Let $u \in V(H)$ and let $v_1, \dots, v_m$ be the neighbours of u. Now construct a graph G by starting with m new vertices $x_1, \dots, x_m$ and n copies $(H_1, \dots, H_n)$ of $H - u$ and, for each $i \in \{1, \dots, m\}$, adding edges connecting x_i to each of the n copies of v_i. Note that G is m-connected and has girth at least g.

Let $w \in V(H) - \{u\}$ and let $x_{m+1}, \dots, x_{m+n}$ be the n copies of w in G. Let $X = \{x_1, \dots, x_{n+m}\}$. It is straightforward to show that there is a unique matroid $M(G; X)$ obtained by extending $M(G)$ by an element e so that, for each subgraph F of G, e is spanned by $E(F)$ if and only there is a component of F that contains X. Moreover, since $g = m + 1$, the matroid $M(G; X)$ is $(m+1)$-connected.

There is a subgroup Γ of $\mathbb{F}_+$ with $|\Gamma| \geqslant 3$ and elements $\alpha(x_1), \dots, \alpha(x_{m-1}) \in \mathbb{F}$ such that no non-empty subsequence of $(\alpha(x_1), \dots, \alpha(x_{m-1}))$ adds to an element of Γ. For each $i \in \{m+1, \dots, m+n\}$, let $\alpha(x_i) \in \Gamma - \{0\}$. Now define $\alpha(x_m)$ so that $\alpha(x_1) + \cdots + \alpha(x_{m+n}) = 0$ and let $\alpha(y) = 0$ for all $y \in V(G) - \{x_1, \dots, x_{m+n}\}$. We let $M(G, \alpha)$ denote the extension of $M(G)$ as described in the previous section. It is easy to verify that $M(G; X) = M(G, \alpha)$. There are $2^n \geqslant c$ different choices of $(\alpha(x_{m+1}), \dots, \alpha(x_{m+n}))$, which proves Theorem 3.1.

References

[1] J. Geelen, G. Whittle, Inequivalent representations of matroids over prime fields, in preparation.

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

[3] J.E. Olsen, A combinatorial problem on finite abelian groups, I, J. Number Theory 1 (1961) 8–10.

[4] J.G. Oxley, Matroid Theory, Oxford University Press, New York, 1992.

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