

On the unique representability of spikes over prime fields

Zhaoyang Wu and Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
wu_zy@nju.edu.cn zwsun@nju.edu.cn

Abstract

For an integer $n \geq 3$, a rank- n matroid is called an n -spike if it consists of n three-point lines through a common point such that, for all $k \in \{1, 2, \dots, n-1\}$, the union of every set of k of these lines has rank $k+1$. Spikes are very special and important in matroid theory. Wu [13] found the exact numbers of n -spikes over fields with 2, 3, 4, 5, 7 elements, and the asymptotic values for larger finite fields. In this paper, we prove that, for each prime number p , a $GF(p)$ representable n -spike M is only representable on fields with characteristic p provided that $n \geq 2p-1$. Moreover, M is uniquely representable over $GF(p)$.

Keywords: Matroid, Spike, Unique Representability

1 Introduction

Spikes are special and important matroids. They are appearing with increasing frequency in the matroid theory literature. Long before the name "spike" was introduced, the Fano and non-Fano matroids, two examples of 3-spikes, had already appeared in almost every corner of matroid theory [6]. Oxley [6, Section 11.2] showed that all rank- n , 3-connected binary matroids without a 4-wheel minor can be obtained from a binary n -spike by deleting at most two elements. Oxley, Vertigan, and Whittle [7] used spikes and one other class of matroids to show that, for all $q \geq 7$, there is no fixed bound on the number of inequivalent $GF(q)$ -representations of a 3-connected matroid, thereby disproving a conjecture of Kahn [4].

Ding, Oporowski, Oxley, and Vertigan [2] showed that every sufficiently large 3-connected matroid has, as a minor, $U_{2,n+2}$, $U_{n,n+2}$, a wheel or whirl of rank n , $M(K_{3,n})$, $M^*(K_{3,n})$, or an n -spike. Moreover, Wu [12] showed that spikes, like wheels and whirls, can be characterized in terms of a natural extremal connectivity condition. Wu [13] discussed the representability of spikes over finite fields, and found the exact numbers of n -spikes over fields with at most seven elements, and the asymptotic values for larger finite fields. One referee for the last mentioned paper was interested in the problem that on what conditions a $GF(p)$ -representable spike is only representable over fields with characteristic p . We consider this problem an interesting one with fair importance in matroid theory, and this paper is a response to the problem.

For $n \geq 3$, a matroid M is called an n -spike with tip t [2] if it satisfies the following three conditions:

- (i) *The ground set is the union of n lines, L_1, L_2, \dots, L_n , all having three points and passing through a common point t ;*

- (ii) $r(\cup_{i=1}^k L_i) = k + 1$ for all $k \in \{1, 2, \dots, n - 1\}$; and
- (iii) $r(L_1 \cup L_2 \cup \dots \cup L_n) = n$.

In this paper, an n -spike with tip t will be simply called an n -spike.

Some 3-spikes have the property that more than one element may be viewed as the tip of the spike. However, it is clear that the tip is unique for an n -spike when $n \geq 4$. Since there are only six 3-spikes, and it is easy to verify all our results for the case $n = 3$, we will assume that n is at least four in the proofs of our lemmas and theorems so that we can fix the tip.

For an n -spike M representable over a field F , if we choose a base $\{1, 2, \dots, n\}$ containing exactly one element from each of the lines L_i , then M can be represented in the form

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ \vdots \\ n \end{array} \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & \dots & 0 & 1 & 1+x_1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 & 1 & 1+x_2 & 1 & \dots & 1 \\ 0 & 0 & 1 & \dots & 0 & 1 & 1 & 1 & 1+x_3 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 1 & 1 & 1 & \dots & 1+x_n \end{array} \right],$$

where the tip of M corresponds to column $n + 1$. We shall call this matrix a *special standard representation* of M and $\{1, 2, \dots, n\}$ the *distinguished basis* associated with the representation. Clearly, this matrix is uniquely determined by the vector (x_1, x_2, \dots, x_n) . We shall call this vector the *diagonal* of the representation.

Two matrix representations A_1 and A_2 are *equivalent* if A_1 can be obtained from A_2 by a sequence of the following six operations. (For details, see [5, Section 6.3].)

- (i) *Interchange two rows.*
- (ii) *Scale a row, that is, multiply it 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) *Scale a column, that is, multiply it by a non-zero member of F .*
- (vi) *Replace each entry of the matrix by its image under some automorphism of F .*

A_1 and A_2 are *weakly equivalent* if we are also allowed to relabel the matroid, that is, A_1 can be obtained from A_2 by a sequence of operations (i) - (vii) where the last of these operations is the following:

- (vii) *Relabel the columns.*

Since our main purpose is to study the conditions on which a matroid is or is not representable over a finite field, we will often consider unlabeled matroids. Thus, we will frequently ignore the labels on elements of matroids, and consider weak equivalence.

If two special standard representations are weakly equivalent, their corresponding diagonals will also be said to be *weakly equivalent*. Two diagonals are *distinct* if they are not weakly

equivalent. Two elements of an n -spike are *conjugate* if they lie on the same line L_i and neither of them is the tip. In a special standard representation of a given spike, if we interchange some base elements with their conjugates, and standardize the resulting matrix, we obtain another special standard representation of the spike. Moreover, all possible special standard representations of the spike are obtainable in this way. In the rest of the paper, we shall call this interchanging-standardizing procedure *swapping*. For two special standard representations A_1 and A_2 of an n -spike, the distinguished bases of $M[A_1]$ and $M[A_2]$ are n -element subsets intersecting all the lines L_i . Since the tip is fixed and is in neither distinguished basis, A_1 and A_2 are weakly equivalent if and only if we can obtain the distinguished basis of $M[A_1]$ from that of $M[A_2]$ by swappings. Therefore, A_1 and A_2 are weakly equivalent if and only if A_1 can be obtained from A_2 by a sequence of swappings, and replacing each entry of the resulting matrix by its image under some automorphism of the field F .

In the rest of this paper, the matroid notation and terminology will follow Oxley [6]. The notation and terminology for spikes will follow Wu [13], of which some results are quoted and some techniques are inherited in this paper.

(1.1) Main Theorem. *For each prime number p , if the integer n is greater than or equal to $2p - 1$, then an n -spike that is $GF(p)$ -representable can only be represented over fields with characteristic p . Moreover, M is uniquely representable over $GF(p)$.*

2 Preliminaries

In the following sections, we use the notation $[m, n]$ to denote the set of consecutive integers from m to n , namely, $\{m, m + 1, m + 2, \dots, n\}$, for our convenience.

(2.1) Lemma. *Let p be a prime integer, n be an integer satisfying the condition $n \geq p - 1$, and $a_1, a_2, \dots, a_n \in GF(p) \setminus \{0\}$. Suppose that $k \in GF(p) \setminus \{0\}$. Then there is a non-empty subset $I \subseteq [1, n]$ such that*

$$\sum_{i \in I} a_i = k.$$

Proof. Viewing $GF(p)$ as $\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$, we rewrite a_i 's as

$$a_i = m_i + p\mathbf{Z},$$

where $1 \leq m_i \leq p - 1$.

As the system $\{i + \frac{p}{m_i}\mathbf{Z}\}_{i=1}^{p-1}$ covers $\{1, 2, \dots, p - 1\}$, but not all the integers, by Theorem 1 of Sun [9] or Corollary 5 of Sun [10], we can not have $|\{\{\sum_{i \in I} \frac{m_i}{p}\} : I \subseteq [1, p - 1]\}| \leq p - 1$. Therefore, $\{\sum_{i \in I} a_i : I \subseteq [1, p - 1]\} = \mathbf{Z}_p$, and the lemma follows. \square

(2.2) Lemma. *Let p be a prime integer, n be an integer satisfying the condition $n \geq p$, and $a_1, a_2, \dots, a_n \in GF(p)$. Then there is a non-empty subset $I \subseteq [1, n]$ such that*

$$\sum_{i \in I} a_i = 0.$$

Proof. Again the lemma can be easily derived from Theorem 1 of Sun [9], and details are thus omitted. \square

The following proposition is not hard to prove by induction. We shall omit the proof.

(2.3) Proposition. *Suppose that n is a positive integer and that $x_i \neq 0$ for all $i \in \{1, 2, \dots, n\}$. Then the determinant of the matrix*

$$\det \begin{pmatrix} 1+x_1 & 1 & 1 & \dots & 1 \\ 1 & 1+x_2 & 1 & \dots & 1 \\ 1 & 1 & 1+x_3 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 1+x_n \end{pmatrix} = [1 + \sum_{i=1}^n x_i^{-1}] \cdot \prod_{i=1}^n x_i.$$

Suppose that A is a special standard representation of an n -spike M over $GF(p)$ with its diagonal $\vec{x} = (x_1, x_2, \dots, x_n)$, and that C is a circuit-hyperplane of M . Suppose that I is the subset of $[1, n]$ such that the elements of M corresponding to $\{x_i | i \in I\}$ is the intersection of C and the set of elements of M to diagonal \vec{x} . Then we deduce by (2.3) that

$$(2.4) \quad \sum_{i \in I} x_i^{-1} = -1.$$

Conversely, suppose that I is a subset of $[1, n]$ such that equality (2.4) holds. Then the elements of M corresponding to $\{x_i | i \in I\}$ combined with the conjugates of the elements corresponding to the remainder of \vec{x} form a circuit-hyperplane of M . Therefore, every circuit-hyperplane C corresponds to an I with $\{x_i | i \in I\}$ satisfying (2.4), and vice versa. We denote the sub-vector corresponding to $\{x_i | i \in I\}$ by $\vec{x}(I)$, and call C the *circuit – hyperplane corresponding to $\vec{x}(I)$* .

(2.5) Proposition. *Let A be a special standard representation of an n -spike M over $GF(p)$ with diagonal $\vec{x} = (x_1, x_2, \dots, x_n)$. Suppose that $n \geq p - 1$. Then \vec{x} is weakly equivalent to a diagonal whose first element is -1 .*

Proof. Since $n \geq p - 1$, we derived from (2.1) that there is a sub-set $I \subseteq [1, n]$ that satisfies (2.4). By weakly equivalence we may assume that there is a positive integer $m \leq n$ such that $I = [1, m]$. Let C be the circuit-hyperplane corresponding to $\vec{x}(I)$. By swapping all but the first element of $\vec{x}(I)$ with their conjugates, we obtain a new special standard representation of M . Let the diagonal of this new special standard representation be $\vec{y} = (y_1, y_2, \dots, y_n)$. It is obvious that for all elements corresponding to \vec{y} only the one corresponding to y_1 is contained in C . The desired result thus follows by (2.3). \square

3 Proof of The Main Theorem

We first introduce the following two propositions.

(3.1) Proposition. *Let p be an odd prime integer, n be an integer with $n \geq 2p - 1$, and matroid M be an n -spike representable over $GF(p)$ and another finite field F with characteristic q . Suppose that A_1, A_2 are two special standard representations of M over $GF(p)$ and F , and their diagonals are $\vec{x} = (-1, x_2, \dots, x_n)$, and $\vec{y} = (y_1, y_2, \dots, y_n)$, respectively. Suppose that $m \in \mathbf{Z} \setminus \{0\}$, and $|m| \leq (p - 1)/2$, and I is a subset of $[2, n]$ such that*

$$|I| \leq p - 1, \text{ and } \sum_{i \in I} x_i^{-1} = m.$$

Then we have the equality

$$\sum_{i \in I} y_i^{-1} = m.$$

Proof. Suppose that C is the circuit-hyperplane corresponding to $x_1 = -1$ of \vec{x} . Since A_1 and A_2 represent the same spike, we deduce by (2.4) that y_1 of \vec{y} is also equal to -1 .

Consider the case that $m = -1$. In this case, since $\sum_{i \in I} x_i^{-1} = -1$, we consider the circuit-hyperplane corresponding to $\vec{x}(I)$. For the reason that A_1 and A_2 are both special standard representation of the same spike, we conclude that $\sum_{i \in I} y_i^{-1} = -1$.

Now consider the case that $m = 1$. Let $K = [2, n] \setminus I$. Since K has at least $p - 1$ elements, we deduce by Lemma (2.1) that there is a subset L of K , such that

$$\sum_{i \in L} x_i^{-1} = -1.$$

Applying a discussion the same as that of the last paragraph, we conclude that

$$\sum_{i \in L} y_i^{-1} = -1.$$

Let $I' = I \cup L \cup \{1\}$. Then we have

$$\sum_{i \in I'} x_i^{-1} = -1.$$

Therefore, there is a circuit-hyperplane C corresponding to $\vec{x}(I')$. Since A_1 and A_2 are both special standard representation of the same spike, we conclude that $\sum_{i \in I'} y_i^{-1} = -1$. It follows that $\sum_{i \in I} y_i^{-1} = 1$.

Using the above result and the same technique, we can now prove Proposition (3.1) for the case $m = -2$. Moreover, it is now clear that we can complete the proof by induction. The details are thus omitted. \square

(3.2) Lemma. *Let p be an odd prime integer, and matroid M be an n -spike representable over $GF(p)$. Suppose that $n \geq 2p - 1$. Then M is uniquely representable over $GF(p)$.*

Proof. Suppose that A_1, A_2 are two special standard representations of M over $GF(p)$, and their diagonals are $\vec{x} = (x_1, x_2, \dots, x_n)$, and $\vec{y} = (y_1, y_2, \dots, y_n)$.

We may assume, by (2.5), that $x_1 = -1$. For singleton set $I = \{i\}$ with $x_i = m, m \in \mathbf{Z} \setminus \{0\}$ with $|m| \leq (p - 1)/2$, we deduce by Proposition (3.1) that $y_i = x_i$. Lemma (3.2) follows immediately. \square

Proof of the Main Theorem Since it is well known that binary spikes are uniquely representable only on fields of characteristic 2, we only need to prove the main theorem with odd prime number p .

Having Lemma (3.2) in hand, we only need to prove that M is not representable over field with characteristic not equal to p . Suppose that F is a field with characteristic q , and M is representable over F . We prove in the following that the prime q must be equal to p .

Suppose that A_1, A_2 are special standard representations of M over $GF(p)$ and F , and $\vec{x} = (x_1, x_2, \dots, x_n)$, and $\vec{y} = (y_1, y_2, \dots, y_n)$ are the diagonals corresponding to A_1 and A_2 , respectively. We assume, as we may, that $x_1 = -1$. Moreover, we use values in $[-\frac{p-1}{2}, \frac{p-1}{2}] \setminus \{0\}$ to represent the value of each x_i^{-1} of \vec{x} . Applying Proposition (3.1), we conclude that, for each $i \in [1, n]$, $y_i^{-1} = x_i^{-1}$ in $GF(q)$. Consequently, M is representable over $GF(q)$, and we may assume that $F = GF(q)$. As a result of the last assumption, we may assume that $q \geq p$ in the following discussion.

Now, consider the subscription set $I = [2, n]$. We partition I into two parts I_+ and I_- , where $I_+ = \{i \in [2, n] : x_i^{-1} > 0\}$, and $I_- = \{i \in [2, n] : x_i^{-1} < 0\}$.

First consider the case that $|I_-| \geq p$. We deduce, by Lemma (2.2), that there is a non-empty subset L of I_- , such that

$$\sum_{i \in L} x_i^{-1} = 0.$$

This equality implies that M has a circuit-hyperplane corresponding to $\vec{x}(L \cup \{1\})$. Since A_2 is also a special standard representation of M , we conclude that the equality

$$\sum_{i \in L} y_i^{-1} = 0$$

holds in $GF(q)$. That is, the equality

$$\sum_{i \in L} x_i^{-1} = 0$$

holds in both $GF(p)$ and $GF(q)$.

Consider the sum $s = \sum_{i \in L} x_i^{-1}$ in \mathbf{Z} . Since all values of x_i^{-1} 's are in $[-\frac{p-1}{2}, -1]$, we have

$$0 > s \geq -\frac{p(p-1)}{2}.$$

Since both p and q are primes, $q \geq p$, and $s = 0$ in $GF(q)$, we conclude that $q = p$.

Now consider the case that $|I_-| \leq p-1$. In this case, we have $|I_+| \geq p-1$. Applying Lemma (2.1), there is a subset J of I_+ , such that

$$\sum_{i \in J} x_i^{-1} = -1.$$

holds in $GF(p)$. This implies that M has a circuit-hyperplane corresponding to $\vec{x}(J)$. Since A_2 is also a special standard representation of M , we conclude that the equality

$$\sum_{i \in J} y_i^{-1} = -1$$

holds in $GF(q)$. That is, the equality

$$\sum_{i \in J} x_i^{-1} + 1 = 0$$

holds in both $GF(p)$ and $GF(q)$.

Consider the sum $s = \sum_{i \in J} x_i^{-1} + 1$ in \mathbf{Z} . Since all values of x_i^{-1} 's are in $[1, \frac{p-1}{2}]$, we have

$$\frac{(p-1)^2}{2} + 1 \geq s > 1.$$

Since both p and q are primes, $q \geq p$, and $s = 0$ in $GF(q)$, we conclude that $q = p$. The main theorem follows immediately. \square

4 Discussion

First we would like to point out that the bound $2p-1$ is sharp for every prime number p . It is easy to prove the following proposition:

(4.1) Proposition *Suppose that M is an n -spike representable over $GF(p)$, and A is a special standard representation of M . Let the diagonal of A be $\vec{x} = (x_1, x_2, \dots, x_n)$. Suppose that*

- (1) $n = 2p - 2$, and

- (2) $x_1 = x_2 = \dots = x_p = -1$, and
- (3) $x_{p+1} = x_{p+2} = \dots = x_{2p-2} = 1$.

Then M is represented by the same matrix A over every prime field $GF(q)$ with $q \geq p$.

Characteristic sets of a matroids had been an interesting topic in matroid theory. The main theorem and proposition (4.1) provide new and interesting examples for the topic. Readers may also discover that some typical examples of this topic are in fact spikes. Besides the Fano and none-Fano matroids, the famous matroids L_p constructed by Lazarsen [5] are also spikes.

An interesting problem related to the main result of this paper is:

(4.2) Problem *What is the lower bound $L(p)$ such that every $GF(p)$ -representable n -spike with $n < L(p)$ is also representable over some fields with characteristic other than p ?*

We do not have the sharp bound for the above problem at current time. Our research shows that $L(p)$ is a number between $\lfloor \log_2(p+2) + 1 \rfloor$, and $\lfloor \log_2(p+2) \rfloor + \lfloor \log_2[4(p+2)/3] \rfloor$. However, the argument is somehow complicated and considered not interesting for our readers. We instead present the following proposition that is related to this problem:

(4.3) Proposition *Suppose that p is an odd prime number, M is an n -spike representable over $GF(p)$, and A is a special standard representation of M . Let the diagonal of A be $\vec{x} = (x_1, x_2, \dots, x_n)$. Let $q = \lfloor \log_2 p \rfloor$. Suppose that*

- (1) $n = 2q + 2$,
- (2) $x_1 = -1$,
- (3) $x_{2^i}^{-1} = -2^{i-1}$, and $x_{2^{i+1}}^{-1} = 2^{i-1}$, for $i \in \{1, 2, \dots, q\}$, and
- (4) $x_{2^{q+2}}^{-1} = -2^q$.

Then M is only representable over fields of characteristic p .

Proof. Suppose that F is a finite field such that M is F -representable. Suppose that A' is a special standard representation of M over F , and its diagonal is $\vec{y} = (y_1, y_2, \dots, y_n)$. By considering the circuit-hyperplane corresponding to $\{x_1\}$, we deduce by applying (2.4) that $y_1 = -1$. Similarly, we have $y_2 = -1$. Next consider the circuit-hyperplane corresponding to the vector (x_1, x_2, x_3) . We conclude again by applying (2.4) that $y_3 = x_3 = 1$. Now switch to consider the circuit-hyperplane corresponding to (x_3, x_4) . We this time conclude that $y_4^{-1} = x_4^{-1} = -2$. For $k \geq 3$, by considering circuit-hyperplanes corresponding to $(x_1, x_{2k-2}, x_{2k-1})$ and $(x_3, x_5, \dots, x_{2k-1}, x_{2k})$ alternatively, it is not hard to derive that

$$y_i^{-1} = x_i^{-1}, \text{ for each } i \in [1, n].$$

Since $q = \lfloor \log_2 p \rfloor$, there is a subset J of $\{2, 4, \dots, 2q + 2\}$ such that

$$\sum_{i \in J} x_i^{-1} = -p \text{ in } \mathbf{Z}.$$

By considering the circuit-hyperplane corresponding to $\vec{x}(J \cup \{1\})$, we conclude that

$$\sum_{i \in J} y_i^{-1} = 0.$$

The last equality implies that equation

$$\sum_{i \in J} x_i^{-1} = -p = 0$$

holds in both fields $GF(p)$ and F . Therefore, F must have characteristic p , and the proposition follows.

References

- [1] G. Ding, B. Oporowski, J.G. Oxley, and D. Vertigan, *Unavoidable minors of large 3-connected matroids*, J. Combin. Theory Ser. B **66** (1996), 334-360.
- [2] G. Ding, B. Oporowski, J.G. Oxley, and D. Vertigan, *Unavoidable minors of large 3-connected binary matroids*, J. Combin. Theory Ser. B **71** (1997), 244-293.
- [3] A. Ingleton, *Representation of matroids*, in: *Combinatorial mathematics and its applications*, Academic Press, London, 1971, pp. 149-167.
- [4] J. Kahn, *On the uniqueness of matroid representations over $GF(4)$* , Bull. London Math. Soc. **20** (1988), 1-12.
- [5] T. Lazarson, *The representation problems of independence functions*, J. London Math. Soc. **33**, 21-25, 1958.
- [6] J.G. Oxley, *Matroid Theory*, Oxford Univ. Press, New York, 1992.
- [7] J. Oxley, D. Vertigan, and G. Whittle, *On inequivalent representations of matroids over finite fields*, J. Combin. Theory Ser. B **67** (1996), 325-343.
- [8] R. Rado, *Note on independence functions*, Proc. London Math. Soc. **7**, 300-320 1957.
- [9] Zhi-Wei Sun, *Covering the integers by Arithmetic Sequences*, Acta Arith. **72**, 109-129, 1995.
- [10] Zhi-Wei Sun, *Covering the integers by Arithmetic Sequences II*, Trans. Amer. Math. Soc. **348**(11), 4279-4320, 1996.
- [11] I. Tomescu, *Introduction to Combinatorics*, Collet's (Publishers) Ltd., London and Wellingborough, 1975.
- [12] Zhaoyang Wu, *On extremal connectivity properties of unavoidable matroids*, J. Combin. Theory Ser. B **75**(1999), 19-45.
- [13] Zhaoyang Wu, *On the number of spikes over finite fields*, Discrete Math. **265** (2003), 261-296.