

## ON THE ALGEBRAIC CHARACTERISTIC SET FOR A CLASS OF MATROIDS<sup>1</sup>

BERNT LINDSTRÖM

**ABSTRACT.** The independent sets of an algebraic matroid are sets of algebraically independent transcendentals over a field  $k$ . If a matroid  $M$  is isomorphic to an algebraic matroid the latter is called an algebraic representation of  $M$ . Vector representations of matroids are defined similarly.

A matroid may have algebraic (resp. vector) representations over fields of different characteristics. The problem in which characteristic sets are possible for vector representations was recently answered (see [2]). The corresponding problem for algebraic representations is open.

We consider a class of matroids  $M_p$  ( $p$  a prime) the vector representations which were determined by T. Lazarsen long ago. One member of this class,  $M_2$ , is the important Fano matroid which plays a crucial role in many parts of matroid theory. We prove that  $M_p$  has algebraic representations only over fields of characteristic  $p$ .

The proof depends on derivations in fields. Using derivations we transform an algebraic representation of  $M_p$  into a vector representation.

We will assume that the reader is familiar with the elements of matroid theory and, in particular, with the notion of an algebraic matroid [5, Chapters 1 and 11].

The matroid  $M_p$  can be defined by its vector representation over the prime field  $\text{GF}(p)$ , the column vectors of the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 1 & 0 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 & 1 & 1 & 1 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 & 1 & 1 & \cdots & 1 & 0 \end{pmatrix}$$

with  $p + 1$  rows and  $2p + 3$  columns. The rank of the matroid  $M_p$  is  $p + 1$ .

Using the vector representation of  $M_p$  it is easy to derive an algebraic representation over  $\text{GF}(p)$  according to [5, Chapter 11.2]. Let  $x_1, x_2, \dots, x_{p+1}$  be algebraically independent transcendentals over  $\text{GF}(p)$ . Let  $y_0 = x_1 + \cdots + x_{p+1}$  and  $y_i = y_0 - x_i$  for  $i = 1, \dots, p + 1$ . The elements of  $M_p$  are then represented by  $x_1, \dots, x_{p+1}, y_0, y_1, \dots, y_{p+1}$  in this order corresponding to the columns of the matrix above.

Of course, there are many other algebraic representations of  $M_p$ . Let me just mention one when  $p = 2$ : replace “+” everywhere in the  $y_i$ ’s by the composition “\*” defined by  $a * b = (a + b)(1 + ab)^{-1}$ . But are there representations of  $M_p$  over

Received by the editors September 6, 1984 and, in revised form, November 11, 1984.

1980 *Mathematics Subject Classification.* Primary 05B35, 12F99.

<sup>1</sup>Research supported by the Swedish Natural Science Research Council.

fields of characteristic distinct from  $p$ ? The problem was suggested for the Fano matroid in [5, Example 11.2.2]. The answer is “no” by our theorem:

**THEOREM.** *If  $M_p$  has an algebraic representation over a field  $k$ , then the characteristic of  $k$  is  $p$ .*

The proof depends on derivations in fields. Let  $k \subseteq E \subseteq F$  be a sequence of field extensions. A *derivation* of  $E$  over  $k$  with values in  $F$  is a mapping  $D: E \rightarrow F$  such that, for any  $x, y \in E$ ,

$$\begin{aligned} D(x + y) &= Dx + Dy, \\ D(xy) &= xDy + yDx, \\ Dx &= 0 \quad \text{if } x \in k. \end{aligned}$$

Using derivations in fields, Ingleton was able to prove in [1] that an algebraic representation over a field of characteristic 0 can be transformed into a vector representation over another field of characteristic 0. Hence any matroid which is algebraic over a field of characteristic 0 is a vector matroid. This does not necessarily hold for prime characteristics. Ingleton’s proof depends on the fact that field extensions are always separable when the characteristic is 0.

An element  $x \in L$  is called *separable* over  $K$  when it is algebraic over  $K$  and its minimal polynomial over  $K$  has distinct roots. An algebraic extension  $L$  of  $K$  is *separable* over  $K$  when each element in  $L$  is separable over  $K$ .

For  $f(X)$  a polynomial in  $K[X]$ , let  $f'(X)$  denote the formal derivative of  $f(X)$ . An irreducible polynomial  $f(X)$  is called *separable* when its root in some extension of  $K$  are distinct. One can prove that  $f(X)$  is separable if and only if  $f'(X)$  is not the zero polynomial [6, p. 49].

If  $a$  is separable algebraic over  $K$ , then any derivation  $D$  of  $K$  over  $k$  has a unique extension to a derivation of  $K(a)$  over  $k$  [6, p. 101]. If  $f^D(X)$  is the result of operating with  $D$  on the coefficients of  $f(X)$ , the minimal polynomial of  $a$  over  $K$ , then  $f^D(a) + f'(a)Da = 0$  gives the value of  $Da$ . More general, if  $L$  is finitely generated and separable algebraic over  $K$ , then any derivative of  $K$  has a unique extension to  $L$ .

If  $K \subset L$  is not a separable extension, it may be impossible to extend a derivation  $D$  of  $K$ . Consider, e.g.,  $k(x^p) \subset k(x)$  when the characteristic is  $p$ , and let  $D(x^p) = 1$  in  $k(x^p)$ .

Assume that  $K = k(x_1, x_2, \dots, x_m)$ , where  $x_1, x_2, \dots, x_m$  are algebraically independent transcendentals over  $k$ .  $K$  is isomorphic to the field of all rational functions of  $m$  variables with coefficients in  $k$ . For  $i = 1, 2, \dots, m$ ,

$$(1) \quad D_i x_j = \delta_{ij}, \quad j = 1, 2, \dots, m,$$

defines a derivation  $D_i$  of  $K$  over  $k$ . If  $r \in K$  then  $D_i r = \partial r / \partial x_i$ , the partial derivative with respect to  $x_i$ . The derivations  $D_1, D_2, \dots, D_m$  are linearly independent over  $K$  and form a base in the vector space  $\text{Der}_k K$  of all derivations of  $K$  over  $k$ . If  $L$  is separable algebraic over  $K$ , then each derivation  $D_i$  has a unique extension  $\bar{D}_i$  to  $L$ , and the derivations  $\bar{D}_1, \dots, \bar{D}_m$  are the base in the vector space  $\text{Der}_k L$  of derivations of  $L$  over  $k$ . The dimension of  $\text{Der}_k L$  is thus  $m =$  the transcendence degree of  $L$  over  $k$ .

For each  $z \in L$  we have a mapping of  $\text{Der}_k L$  into  $L$  which maps  $D \in \text{Der}_k L$  on  $Dz$ . This map, which is a linear functional on the vector space  $\text{Der}_k L$ , is denoted

by  $dz$ . By (1) it follows that  $dx_1, dx_2, \dots, dx_m$  are linearly independent. Also note that (cf. [3, p. 269])

$$d(xy) = xdy + ydx, \quad d(x + y) = dx + dy.$$

We intend to use the operator  $d$  to transform algebraic representations of matroids into vector representations. But some caution is necessary.

EXAMPLE. Consider the matroid with the algebraic representation  $x, y, z, xy, xz, yz$  over  $\text{GF}(p)$ , where  $x, y, z$  are algebraically independent transcendentals over  $\text{GF}(p)$ . Note that  $xy, xz, yz$  are algebraically independent over  $\text{GF}(p)$ . Also note that different  $\text{GF}(p)$  give isomorphic matroids. We now apply the operator  $d$ . We get  $dx, dy, dz, xdy + ydx, xdz + zdx, ydz + zdy$  over  $\text{GF}(p)$ . The last three elements are linearly independent if and only if  $p \neq 2$ . This shows that new circuits may appear which were not there before the application of the operator  $d$ .

PROOF OF THE THEOREM. Assume w.l.o.g. that  $k$  is algebraically closed. Let  $x_1, \dots, x_{p+1}, y_0, y_1, \dots, y_{p+1}$  be an algebraic representation of  $M_p$  over a field  $k$  of characteristic  $q$ —we use the same letters as before in order to facilitate identification. In particular,  $x_1, \dots, x_{p+1}$  will correspond to a base of  $M_p$  and are therefore algebraically independent over  $k$ . We want to prove that  $q = p$ .

We shall prove that there are numbers  $m_1, \dots, m_{p+1}$  and  $n_0, \dots, n_{p+1}$ , which are powers of  $q$ , for which  $y^{n_i}$  is separable algebraic over  $k(x_1^{m_1}, \dots, x_{p+1}^{m_{p+1}})$  when  $i = 0, 1, \dots, p + 1$ . To simplify, write  $x_i^{m_i} = \xi_i$  and  $y_j^{n_j} = \eta_j$ . Let  $K = k(\xi_1, \dots, \xi_{p+1})$  and  $L = K(\eta_0, \dots, \eta_{p+1})$ . Then  $L$  is separable algebraic over  $K$ . Hence, any derivation  $D$  on  $K$  over  $k$  has a unique extension  $\bar{D}$  on  $L$ . The dual vector space  $(\text{der}_k L)^*$  has the base  $d\xi_1, \dots, d\xi_{p+1}$ .

When we apply the operator  $d$  the algebraic representation of  $M_p$  is transformed into a vector representation of a matroid  $M'_p$ , which a priori may be nonisomorphic to  $M_p$  (in fact, they are isomorphic when  $q = p$ ). It is important that the following circuits are preserved when the operator  $d$  is applied:

$$\begin{aligned} A &= \{x_1, x_2, \dots, x_{p+1}, y_0\}, \\ B_i &= \{x_1, \dots, x_{i-1}, y_i, x_{i+1}, \dots, x_{p+1}\}, \quad i = 1, \dots, p + 1, \\ C_i &= \{x_i, y_0, y_i\}, \quad i = 1, \dots, p + 1, \\ E &= \{y_1, \dots, y_{p+1}\}. \end{aligned}$$

The verification that these are circuits of  $M_p$  is left for the reader.

Since  $A$  is a circuit there is a polynomial  $A(X_1, \dots, X_{p+1}, Y_0)$  with coefficients in  $k$  for which  $A(x_1, \dots, x_{p+1}, y_0) = 0$ . Choose  $A$  of minimum total degree (the total degree of a polynomial is the sum of degrees of all monomials which occur in the polynomial) such that for  $m_1, \dots, m_{p+1}, n_0$ , which are powers of  $q$ ,

$$(2) \quad A(x_1^{m_1}, \dots, x_{p+1}^{m_{p+1}}, y_0^{n_0}) = 0.$$

For brevity we shall denote partial derivatives of a polynomial  $A$  by  $A^i = \partial A / \partial X_i$  ( $1 \leq i \leq p + 1$ ),  $A^{p+2} = \partial A / \partial Y_0$ . We now claim that

$$(3) \quad A^i(x_1^{m_1}, \dots, x_{p+1}^{m_{p+1}}, y_0^{n_0}) \neq 0, \quad i = 1, \dots, p + 2.$$

Assume w.l.o.g. that  $A^1 = 0$ . If  $A^1$  is the zero polynomial then we can find a polynomial  $P$  with  $P(X_1^q, X_2, \dots, Y_0) = A(X_1, \dots, Y_0)$ , hence  $P(x_1^{qm_1}, \dots, x_{p+1}^{m_{p+1}}, y_0^{n_0}) =$

0. Note that  $P$  has smaller total degree than  $A$ , since all variables do occur. This is a contradiction by the choice of  $A$ . Hence  $A^1$  is not the zero polynomial. If  $A^1(x_1^{m_1}, \dots, x_{p+1}^{m_{p+1}}, y_0^{n_0}) = 0$  then we have a contradiction since the polynomial  $A^1$  has smaller total degree than  $A$ . Therefore (3) holds.

Since  $B_i$  is a circuit, we can find a polynomial  $B_i$  and a number  $n_i$ , which is a power of  $q$ , where  $B_i$  has minimum total degree with

$$(4) \quad B_i(x_1^{m_1}, \dots, y_i^{n_i}, \dots, x_{p+1}^{m_{p+1}}) = 0, \quad i = 1, \dots, p + 1.$$

We do not exclude fractional  $n_i$  ( $q$ th roots). Since  $B_i$  has minimum total degree, we conclude as before that

$$(5) \quad B_i^i(x_1^{m_1}, \dots, y_i^{n_i}, \dots, x_{p+1}^{m_{p+1}}) \neq 0, \quad i = 1, \dots, p + 1,$$

where  $B_i^i$  is the partial derivative of  $B_i$  with respect to  $Y_i$ .

At least one more derivative is nonzero:

$$(6) \quad \exists j: j \neq i, \quad B_i^j(x_1^{m_1}, \dots, y_i^{n_i}, \dots, x_{p+1}^{m_{p+1}}) \neq 0, \quad i = 1, \dots, p + 1.$$

Assume that all  $j$ th derivatives are 0 when  $j \neq i$ . Then we can find  $h_j = q^{c_j}$ ,  $c_j \geq 1$  ( $j \neq i$ ) and a polynomial  $H_i$  over  $k$  such that

$$B_i(X_1, \dots, Y_i, \dots, X_{p+1}) = H_i(X_1^{h_1}, \dots, Y_i, \dots, X_{p+1}^{h_{p+1}}).$$

Then there is a polynomial  $K_i$  such that

$$B_i(X_1, \dots, Y_i^q, \dots, X_{p+1}) = (K_i(X_1, \dots, Y_i, \dots, X_{p+1}))^q,$$

and we have, by (4),

$$K_i(x_1^{m_1}, \dots, y_i^{n_i/q}, \dots, x_{p+1}^{m_{p+1}}) = 0.$$

Since  $K_i$  has smaller total degree than  $B_i$ , we have a contradiction, and (6) follows.

For brevity we will write  $x_i^{m_i} = \xi_i$  ( $1 \leq i \leq p + 1$ ),  $y_i^{n_i} = \eta_i$  ( $0 \leq i \leq p + 1$ ). Note that  $\eta_i$  is separable algebraic over  $K = k(\xi_1, \xi_2, \dots, \xi_{p+1})$ , which is purely transcendental over  $k$ , by (2)–(5). Let  $L = K(\eta_0, \dots, \eta_{p+1})$ . Then  $L$  is separable algebraic over  $K$ . Let  $d$  be the operator which associates an  $L$ -linear functional  $dz \in (\text{der}_k L)^*$  with  $z \in L$ .

Because of the circuit  $C_i$  there is a polynomial  $C_i$  of minimum total degree such that

$$(7) \quad C_i(\xi_i, \eta_0, \eta_i) = 0, \quad i = 1, \dots, p + 1.$$

At least one partial derivative  $C_i^j$  ( $j = 1, 2, 3$ ) is nonzero:

$$(8) \quad \exists j \in \{1, 2, 3\}: C_i^j(\xi_i, \eta_0, \eta_i) \neq 0.$$

We prove later that all three derivatives are nonzero.

If we apply the operator  $d$  to (2), (4) and (7), we find

$$(9) \quad \sum_{j=1}^{p+1} A^j d\xi_j + A^{p+2} d\eta_0 = 0,$$

$$(10) \quad \sum_{j \neq i, j=1}^{p+1} B_i^j d\xi_j + B_i^i d\eta_i = 0, \quad i = 1, \dots, p + 1,$$

$$(11) \quad C_i^1 d\xi_i + C_i^2 d\eta_0 + C_i^3 d\eta_i = 0, \quad i = 1, \dots, p+1.$$

We eliminate  $d\eta_0$  between (9) and (11), and find

$$(12) \quad (A^i C_i^2 - A^{p+2} C_i^1) d\xi_i - A^{p+2} C_i^3 d\eta_i + \sum_{j \neq i, j=1}^{p+1} A^j C_i^2 d\xi_j = 0.$$

We will prove that  $C_i^j(\xi_i, \eta_0, \eta_i) \neq 0$  for  $j = 1, 2, 3$ . Assume that  $C_i^3(\xi_i, \eta_0, \eta_i) = 0$ . Then we have a nontrivial linear relation between  $d\xi_1, \dots, d\xi_{p+1}$  by (3), (8) and (12), which is impossible. Hence  $C_i^3 \neq 0$ .

Next we find by (5), (10) and (12),

$$(13) \quad A^i C_i^2 = A^{p+2} C_i^1.$$

By (13) and (3) it follows that  $C_i^1$  and  $C_i^2$  are either both 0 or distinct from 0. In the first case we find by (12)  $d\eta_i = 0$ , and we have a nontrivial linear relation between  $d\xi_1, \dots, d\xi_{p+1}$  by (6) and (10). This is impossible. Therefore we have

$$(14) \quad C_i^j(\xi_i, \eta_0, \eta_i) \neq 0, \quad j = 1, 2, 3; \quad i = 1, \dots, p+1.$$

By (12), (3) and (14) we then find

$$(15) \quad A^{p+2} C_i^3 (C_i^2)^{-1} d\eta_i = \sum_{j \neq i, j=1}^{p+1} A^j d\xi_j, \quad i = 1, \dots, p+1.$$

We recall that  $E = \{y_1, \dots, y_{p+1}\}$  is a circuit of  $M_p$ . This implies a nontrivial linear relation between  $d\eta_1, \dots, d\eta_{p+1}$ , and the right-hand members of (15) ( $i = 1, \dots, p+1$ ) have to be linearly dependent. The determinant of the system is  $pA^1 \cdots A^{p+1}$ , which is 0 only when  $p = 0$ . Hence the characteristic is  $p$ , which was to be proved.

REMARK. When the characteristic of  $k$  is  $p$  then (9) and (15) give a vector representation of  $M_p$ , which is the first mentioned representation of  $M_p$  in some disguise.

## REFERENCES

1. A. W. Ingleton, *Representations of matroids*, Combinatorial Mathematics and its Applications (D. J. A. Welsh, ed.), Academic Press, London and New York, 1971, pp. 149-169.
2. J. Kahn, *Characteristic sets of matroids*, J. London Math. Soc. **26** (1982), 207-217.
3. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1971.
4. T. Lazarsen, *The representation problem for independence functions*, J. London Math. Soc. **33** (1958), 21-25.
5. D. J. A. Welsh, *Matroid theory*, Academic Press, London, 1976.
6. D. J. Winter, *The structure of fields*, Springer-Verlag, New York-Heidelberg-Berlin, 1974.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF STOCKHOLM, BOX 6701, S-113 85 STOCKHOLM, SWEDEN