Riv. Mat. Univ. Parma (4) **14** (1988), 151-156

DĂNUŢ MARCU (*)

Note on the algebraic matroids (**)

Introduction

When we use the word *geometry*, we mean an independence structure with the exchange property on a possible infinite set. We shall call *matroid*, a geometry on a finite set.

Let F be a field and K an extension of F. Algebraic independence in K over F gives a geometry. If F and K are algebraically closed fields, we have a *full algebraic geometry* or FAG, for brevity.

The *points* in a FAG have the form $\overline{F(x)}$, where x is transcendental over F and the bar denotes algebraic closure.

The *lines* of a FAG have the form $\overline{F(x, y)}$, where x and y are algebraically independent transcendentals over F. More generally, a flat of rank r has the form $\overline{F(x_1, \ldots, x_r)}$, with $x_1, \ldots, x_r$ algebraically independent over F.

Lindström [5]$_1$ did prove the converse of Desargues' Theorem for FAG's, by applying a Lemma of Ingleton and Main [3]. The Ingleton-Main Lemma was generalized by Dress and Lovász [2] (for full algebraic matroids) to the Series Reduction Theorem, and a further generalization gave the concept of *pseudomodular lattice*, in the paper of Björner and Lovász [1]. Among many equivalent formulations for *pseudomodularity* of a semimodular lattice, we choose one which comes quite close to the Ingleton-Main Lemma: let u, v, w be flats in the lattice and assume that u covers $u \wedge w$ and v covers $v \wedge w$. Then, $r(u \wedge v) - r(u \wedge v \wedge w) \leqslant 1$.

The Ingleton-Main Lemma is the special case $r(u) = r(v) = r(w) = 3$. The proof that we shall give of pseudomodularity for FAG's is elementary and is constructive.

(*) Indirizzo: Str. Pasului 3, Sect. 2, R-70241-Bucharest.

(**) Ricevuto: 24-V-1988.

1 – In the sequel, I denotes one of the rings Z or $GF(p)$, for a prime p.

A main tool in the proofs will be the following result ([7], Theorem 1 or [4], Theorem 5.6).

Seidenberg's Theorem. Consider a system

$$F_1 = 0, \ldots, F_s = 0 \qquad G \neq 0 \tag{1}$$

where the F_i and G are elements of the ring $I[a_1, \ldots, a_m; X_1, \ldots, X_n]$. There exists a finite number of systems

$$f_{j1} = 0, \ldots, f_{js_j} = 0 \qquad g_j \neq 0 \tag{R$_j$}$$

where f_{jk} and g_j are elements in the ring $I[a_1, \ldots, a_m]$, having the following property: for any field K containing I, any extension field L of K and any values $\overline{a}_i$ in K of the a_i, the system $(\overline{1})$, obtained from (1) by replacing the a_i by $\overline{a_i}$, has a solution in some algebraic extension field of L if and only if for at least one j the $\overline{a_i}$ form a solution of (R_j).

Moreover, the (R_j) can be computed within a finite number of steps, depending only on the F_i and G.

Before we give the proof of Piff's Conjecture, we would like to discuss a simple example, which is much of a clue to the proof.

Example. We consider a matroid of rank 2 with three elements x, y, z which form a circuit of the matroid. Hence, all 2-sets are bases of the matroid. For an algebraic representation of this matroid, let x and y be algebraically independent over $F(t)$ and let the third element z satisfy the equation $z^2 - (x+y)z + (1-t)xy = 0$. It is not hard to see that this gives an algebraic representation of the matroid. Suppose we wish to substitute a number for t from F or an algebraic extension of F; we want another algebraic representation of the matroid, if possible one over F.

Question. Which numbers should be avoided, and how do we find them?

Guess. Choose t, such that coefficients do not disappear. If we substitute 0 for t, we shall get $z^2 - (x+y)z + xy = 0$. Hence, $z = x$ or y. Not the same matroid!

Another guess. Choose t, such that the polynomial becomes irreducible over $F(x, y)$. Wrong again! Take $t = 1$; $z = x + y$ is acceptable.

In fact, it turns out that $t = 0$ is the only exceptional value. How do we find it?

Suppose we postulate that x and y are algebraically independent transcendentals over $F(t)$. Solving the equation in x, we get $x = (z^2 - yz)/(z - (1-t)y)$. Hence, x and y are in the algebraic closure of the field $F(t)(y, z)$. This implies that y and z are algebraically independent over $F(t)$. Similarly, we can prove that x and z are independent. There are two restrictions: $z - (1-t)y \neq 0$ and $z - (1-t)x \neq 0$, which contain the unknown z. By using Seidenberg's Theorem, we can eliminate z and get conditions of the form $f_{ij}(t, x, y) = 0$, $g_j(t, x, y) \neq 0$. The first one is an identity; it can be dropped.

The second one, $g_j(t, x, y) \neq 0$, gives a necessary and sufficient condition for the existence of z, such that x, y, z will be an algebraic representation of the matroid. Hence, we choose a number α, such that $g_j(\alpha, x, y) \neq 0$. It may be necessary to choose α in an algebraic extension of F, if F is finite. Then, we apply the following lemma of Piff [**6**].

Lemma. *If a matroid M is algebraic over $F(\alpha)$, where α is algebraic over F, then M is algebraic over F.*

Proof. Consider a circuit $\{a_1, \ldots, a_n\}$ in the algebraic matroid M over $F(\alpha)$. Then, we have $P(a_1, \ldots, a_n) = 0$, for some non zero polynomial $P(X_1, \ldots, X_n)$ over $F(\alpha)$. It follows that a_1 is algebraic over $F(\alpha, a_2, \ldots, a_n)$. Since α is algebraic over F, it follows that a_1 is algebraic over $F(a_2, \ldots, a_n)$. There exists, therefore, a polynomial $Q(X_1, \ldots, X_n)$, over F, such that $Q(a_1, \ldots, a_n) = 0$.

2 - The main results

The following result was conjectured by Piff [**6**].

Theorem 1. *Assume that the matroid M is algebraic over a field $F(t)$, where t is transcendent over F. Then, M is algebraic over F.*

Proof. Let $x_1, \ldots, x_r$ be a fixed basis of the algebraic matroid M over $F(t)$. Let $y_1, \ldots, y_n$ be the remaining elements of the matroid. For each circuit C of the matroid, there exists a polynomial $P_C(X_1 \ldots, X_r, Y_1, \ldots, Y_n)$, over $F(t)$, such that $P_C(x_1, \ldots, x_r, y_1, \ldots, y_n) = 0$. The polynomial P_C contains, explicitely, only those variables which correspond to elements of C. Let $K_C \in F(t)$ be the coefficient of a non constant term in P_C.

For each basis B of M and each x_i not in B, there exists a fundamental circuit $C = C(x_i, B)$, containing x_i and some elements from B. Let $K_{C,i}$ be the coefficient of the highest power of X_i of the polynomial P_C, regarded as a polynomial in the variable X_i. $K_{C,i}$ is a polynomial in the variables which correspond to the elements of $B \cap C$. The set of all circuits in M is denoted by $\mathcal{C}$. The subset of circuits of type $C(x_i, B)$ is denoted by $\mathcal{D}$.

Any solution $X_1 = x_1, \ldots, Y_n = y_n$, with $x_1, \ldots, x_n$ algebraically independent over $F(t)$, to the system of equations and inequations $P_C(X_1, \ldots, Y_n) = 0$, $K_C \neq 0$ for $C \in \mathcal{C}$ and $K_{C,i} \neq 0$ for $C \in \mathcal{D}$ will be an algebraic representation of M over $F(t)$. This is also true, if we substitute a number in some algebraic extension of F for t (we may assume that all coefficients belong to $F[t]$).

The condition $K_C \neq 0$ implies that the polynomial $P_C \neq 0$, after such a substitution, and the elements of C will be a dependent set in the new representation. The condition $K_{C,i} \neq 0$ implies that x_i is algebraic over the field $F(t)(B)$, when $1 \leqslant i \leqslant r$, and B will become algebraically independent over $F(t)$, since it is a basis.

We may regard $t, X_1, \ldots, X_r$ as parameters and eliminate $Y_1, \ldots, Y_n$, by the theorem of Seidenberg, applied to the above system of equations and inequations. Then, we get a finite collection of systems $(\mathrm{R_j})$ of equations and inequations, with the f_{jk} and g_j polynomial functions of the parameters. For at least one j, $(\mathrm{R_j})$ has a solution $X_1 = x_1, \ldots, X_r = x_r$. The equalities $f_{jk} = 0$ are necessarily identities in t. Only the inequality $g_j \neq 0$ gives a restriction on t. It is clear that we can find a number α in some algebraic extension of F, such that $g_j \neq 0$, when this number is substituted for t. It follows then, by Seidenberg's Theorem, that the first system of equations and inequations has a solution $Y_1 = y_1, \ldots, Y_n = y_n$, in some algebraic extension of $F(\alpha)(x_1, \ldots, x_r)$. Therefore, we have an algebraic representation of the matroid over $F(\alpha)$ and, then, also over F, by Piff's Lemma.

Theorem 2. *Full algebraic combinatorial geometries* (FAG'S) *have the pseudomodular property.*

Proof. Let u, v, w be flats of a FAG, such that u covers $u \wedge w$, v covers $v \wedge w$ and $r(u \wedge v) - r(u \wedge v \wedge w) \geqslant 2$. This will give a contradiction and the theorem follows.

We may assume that $w = (u \wedge w) \vee (v \wedge w)$. For, in other case, we may use $(u \wedge w) \vee (v \wedge w)$ as a new w, and coverings are preserved and the inequality also in the assumptions. Since $r(u \wedge v) - r(u \wedge v \wedge w) \geqslant 2$, we can find two numbers x,

y in the field $u \wedge v$, algebraically independent over the field $u \wedge v \wedge w$. Let $A \subset u \wedge w$ and $B \subset v \wedge w$ be maximal subsets, algebraically independent over the field $u \wedge v \wedge w$.

Since u covers $u \wedge w$ and v covers $v \wedge w$, it follows that $A \cup \{x, y\}$ and $B \cup \{x, y\}$ are algebraically dependent over the field $u \wedge v \wedge w$. Write $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ (A and B are non zero). Now, there are non zero polynomials $P(X, Y, X_1, \ldots, X_m)$ and $Q(X, Y, Y_1, \ldots, Y_n)$, over the field $u \wedge v \wedge w$, such that $P(x, y, a_1, \ldots, a_m) = 0$ and $Q(x, y, b_1, \ldots, b_n) = 0$.

P and Q contain the variables X and Y, explicitely, since x and y are transcendentals over $u \wedge w$ and $v \wedge w$ (x, y belong to $u \wedge v$ and are transcendental over $u \wedge v \wedge w$). Since A and B are algebraically independent over the field $u \wedge v \wedge w$, we have $P(X, Y, a_1, \ldots, a_m) \neq 0$ and $Q(X, Y, b_1, \ldots, b_n) \neq 0$. Let C_P and C_Q be the coefficients of the highest power of X in P and Q, respectively. Let $C(X, Y)$ be the coefficient of a non constant term in $P(X, Y, X_1, \ldots, X_m)$, regarded as a polynomial in the X_i's.

Now, $X = x$, $Y = y$, $X_1 = a_1, \ldots, X_m = a_m$, $Y_1 = b_1, \ldots, Y_n = b_n$ is a solution to the system of equations and inequations

$$P(X, Y, X_1, \ldots, X_m) = 0 \qquad Q(X, Y, Y_1, \ldots, Y_n) = 0$$

$$C_P(Y, X_1, \ldots, X_m) \neq 0 \qquad C_Q(Y, Y_1, \ldots, Y_n) \neq 0 \qquad C(X, Y) \neq 0.$$

If we eliminate X, we obtain, by Seidenberg's Theorem, a finite number of systems (R_j): $f_{j1} = \ldots = f_{js_j} = 0$, $g_j \neq 0$. At least (R_j) has a solution $Y = y$, $X_i = a_i$ $(1 \leqslant i \leqslant m)$, $Y_j = b_j$ $(1 \leqslant j \leqslant n)$. If Y appears explicitely in the polynomial f_{jk}, it follows that $y \in (u \wedge w) \vee (v \wedge w) = w$, which is a contradiction. Hence, the variable Y does not appear explicitely in the polynomials f_{jk}. Therefore, we can find $b \in F$, such that, by Seidenberg's Theorem, the system

$$P(X, b, a_1, \ldots, a_m) = 0 \qquad Q(X, b, b_1, \ldots, b_n) = 0$$

$$C_P(b, a_1, \ldots, a_m) \neq 0 \qquad C_Q(b, b_1, \ldots, b_n) \neq 0 \qquad C(X, b) \neq 0$$

has a solution $X = a$, in some field. By the first four of these relations, we find that $a \in (u \wedge w) \wedge (v \wedge w) = u \wedge v \wedge w$.

Note that $P(a, b, a_1, \ldots, a_m) = 0$ and $P(a, b, X_1, \ldots, X_m) \neq 0$, since $C(a, b) \neq 0$. This implies that $\{a_1, \ldots, a_m\}$ is algebraically dependent over the field $u \wedge v \wedge w$, which is a contradiction.

We think that this proof is an interesting application of the Theorem of Seidenberg.

Acknowledgement. I wish to thank the referee for his helpful comments, kindness and interest concerning this paper.

References

[1] A. BJÖRNER and L. LOVÁSZ, *Pseudomodular lattices and continuous matroids*, Department of Mathematics, University of Stockholm, Report No. 4, 1987.

[2] A. DRESS and L. LOVÁSZ, *On some combinatorial properties of algebraic matroids*, Combinatorica 7 (1987), 39-48.

[3] A. W. INGLETON and R. A. MAIN, *Non-algebraic matroids exist*, Bull. London Math. Soc. 7 (1975), 144-146.

[4] N. JACOBSON, *Basic Algebra*, Freeman & Co., New York, 1985.

[5] B. LINDSTRÖM: $[\bullet]_1$ *A desarguesian theorem for algebraic combinatorial geometries*, Combinatorica 5 (1985), 237-239; $[\bullet]_2$ *A reduction of algebraic representations of matroids*, Proc. Amer. Math. Soc. **100** (1987), 388-389.

[6] M. J. PIFF, *Some problems in combinatorial theory*, Ph. D. Thesis, Oxford, 1972.

[7] A. SEIDENBERG, *Some remarks on Hilbert's nullstellensatz*, Arch. Math. 7 (1956), 235-240.

[8] O. V. SHAMEYEVA, *On the algebraic representability of matroids* (in Russian), Vestnik Moskovskogo Universiteta, Matematika 4 (1985), 29-32.

Résumé

Dans ce travail, nous démontrons la conjecture de Piff [6] *et nous donnons une nouvelle démonstration de la sémimodularité des matroïdes algébriques.*

***