COMBINATORICA 7 (1) (1987) 39—48

ON SOME COMBINATORIAL PROPERTIES OF ALGEBRAIC MATROIDS

A. DRESS and L. LOVÁSZ

Received 23 November 1984
Revised 15 November 1985

It was proved implicitly by Ingleton and Main and explicitly by Lindström that if three lines in the algebraic matroid consisting of all elements of an algebraically closed field are not coplanar, but any two of them are, then they pass through one point. This theorem is extended to a more general result about the intersection of subspaces in full algebraic matroids. This result is used to show that the minimax theorem for matroid matching, proved for linear matroids by Lovász, remains valid for algebraic matroids.

0. Introduction

One of the sources of matroid theory was the observation of van der Waerden in the second edition of his "Moderne Algebra" [9] that linear and algebraic independence satisfy the same combinatorial "exchange rules". It is surprising then that while linear matroids have been studied to a very large extent, from geometric, combinatorial as well as algorithmic point of view, very little is known about algebraic matroids. Ingleton and Main [1] proved that non-algebraic matroids exist by showing that the Vamos matroid was non-algebraic. Recently Lindström [3, 4] revived the subject by settling several of the unsolved problems concerning algebraic representations of matroids. Among others, he proved that the "non-Pappus" matroid in algebraic but the "non-Desargues" matroid is not.

An important tool in the study of linear matroids is the fact that they can be embedded into the matroid formed by *all* elements in a linear (or projective) space. The lattice of subspaces of this full linear space is *modular*. This fact compresses a number of important geometric facts about subspaces, such as "two lines in a plane have a point is common", "two planes in a rank 4 space have a line in common" etc.

For algebraic matroids, there also exists a natural notion of "fullness": this is the algebraic matroid formed by all elements of an algebraically closed field. However, the lattice of algebraically closed subfields of such a field (i.e. the lattice of flats of this matroid) is *not* modular, and so we loose the nice geometric facts mentioned above. But some of the geometry can be salvaged. The following lemma, which is implicit in the paper of Ingleton and Main [1], plays an important role in the investigations of Lindström:

AMS subject classification (1980): 05 B 35

Ingleton—Main Lemma. *Let e_1, e_2 and e_3 be three lines in a full algebraic matroid. Suppose that e_1, e_2 and e_3 are not coplanar but any two of them are. Then e_1, e_2 and e_3 have a point in common.* ∎

In this paper we prove some generalizations of this property of full algebraic matroids. Our main result (Theorem 1.2) says that any set of elements which are in series in some set can be replaced by a single element which is still in the full algebraic matroid.

Let $\mathcal{H}$ be a collection of lines in a matroid. We say that $\mathcal{H}$ is a *matching* if $r(\bigcup\mathcal{H})=2|\mathcal{H}|$ (equivalently, if choosing two non-parallel points from every line in $\mathcal{H}$, we obtain an independent set). The *matroid matching problem* is the following: given any family $\mathcal{H}$ of lines in a matroid, find a largest subfamily forming a matching. This problem contains a number of combinatorial optimization problems as special cases, most notably the matching problem for graphs and the matroid intersection problem (see e.g. Lovász [6]). Unfortunately, this problem cannot, in general, be solved in polynomial time (Jensen and Korte [2], Lovász [8]).

However, in the special case when the underlying matroid is a full linear space, a minimax formula (Lovász [5]) as well as a polynomial-time algorithm (Lovász [7]) can be derived. The key property of full linear matroids used in these studies turns out to be equivalent to one of the generalizations of the Ingleton-Main lemma. Hence we can extend the min-max formula for matroid matching from linear to algebraic matroids.

There are other classes of matroids which have a natural notion of "fullness". We study complete graphs and full transversal matroids and show that a generalized Ingleton—Main lemma remains valid for them too. This implies that the min—max formula for matroid matching can also be extended; this illuminates why the matroid matching problem has been found easier for graphic and transversal matroids (Lovász [6], Po Tong, Lawler and Vazirani [8]).

It is likely that the matroid matching *algorithm* can also be extended to algebraic matroids. This, however, requires a more thorough study of algorithmic aspects of algebraic matroids: how are they given and how are basic operations, like testing for algebraic independence, carried out? We do not go into the details of these interesting questions in this paper.

Acknowledgement. The authors are grateful to the referee for pointing out an error in an earlier version and for suggesting several improvements.

1. The generalized Ingleton—Main lemma

Let F and K be two fields such that $F\subset K$. Assume that F and K are algebraically closed and K has finite transcendence degree over F. Then those subfields of K which are algebraically closed and contain F form the flats of a matroid. A set $A\subseteq K$ is independent in this matroid if and only if its elements are algebraically independent over F. We call this matroid the *full algebraic matroid* $A(K/F)$. Adopting the usual language of matroid theory, flats (i.e. algebraically closed subfields) of transcendence degree 1 are called *points*, flats of transcendence degree 2 are called *lines* etc.

A matroid which is isomorphic to a restriction of $A(K/F)$ is called *algebraic over* F.

We denote by $\mathrm{cl}_F(X)$ the algebraic closure of $F[X]$, and by $\mathrm{tr}_F(X)$ or simply $\mathrm{tr}(X)$ the transcendence degree of X over F.

Next we need some discussion of the representation of algebraic matroids. The usual definition is that for any matroid $(E; r)$, an *algebraic representation* in the field K over the field F is a mapping $\delta: E \to K$ such that $r(X) = \mathrm{tr}(\delta(X))$ for every $X \subseteq E$.

At a first glance, this representation cannot even be described in finite space. But we may observe the following. The mapping δ induces a homomorphism of the polynomial ring $F[X_e : e \in E]$ into K (over F), and hence it can be described by its kernel, which is a polynomial ideal I_δ.

Let us introduce the following notation: if $A = \{a_1, \dots, a_k\} \subseteq E$ then we set $X_A = (X_{a_1}, \dots, X_{a_k})$. Then

$$\mathcal{M} = \{A \subseteq E:\ I_\delta \cap F[X_A] = \{0\}\}$$

is isomorphic to the algebraic matroid defined by δ. Since according to Hilbert, this ideal can always be described by a finite number of generators, this yields a finite description of an algebraic matroid. In fact, to define the matroid it suffices to specify, for each circuit C, a polynomial $p_C \in I_\delta \cap F[X_C]$. If we replace I_δ by the ideal generated by the polynomials p_C in the formula for $\mathcal{M}$ above, then we obtain the same matroid. This description of the matroid still uses exponentially many polynomials. It can be argued that $O(|E|)$ polynomials already define $(E, \mathcal{M})$; but we do not go into the details of this.

Note that the polynomial p_C can be chosen irreducible over F. We shall it the *polynomial associated with* c. The next lemma describes all circuits with a given associated polynomial.

Lemma 1.0. *Let* $p \in F[X_1, \dots, X_k]$ *be irreducible over* F *and let* $\delta_1, \dots, \delta_k \in K$ *such that* $p(\delta_1, \dots, \delta_k) = 0$ *and* $\mathrm{tr}\{\delta_1, \dots, \delta_k\} = k-1$. *Suppose that each* x_i *occurs in* p *explicitly. Then* $\{\delta_1, \dots, \delta_k\}$ *is a circuit in* $\mathcal{A}(K/F)$.

Proof. Since $\mathrm{tr}\{\delta_1, \dots, \delta_k\} = k-1$, it follows by elementary matroid theory that $\{\delta_1, \dots, \delta_k\}$ contains a unique circuit, say $\{\delta_1, \dots, \delta_r\}$. We want to show that $r = k$. Suppose not. Let $q \in F[X_1, \dots, X_r]$ be an irreducible polynomial associated with the circuit $\{\delta_1, \dots, \delta_r\}$. Consider the polynomials $p' = p|_{x_2=\delta_2, \dots, x_k=\delta_k} \in K[X_1]$ and $q' = q|_{x_2=\delta_2, \dots, x_r=\delta_r} \in K[X_1]$. Since $\delta_2, \dots, \delta_k$ are algebraically independent, it follows that p' and q' are irreducible over $F(\delta_2, \dots, \delta_k)$ (cf. Van der Waerden [9]). But p' and q' have the root $x_1 = \delta_1$ in common, and hence there is a $\lambda \in F(\delta_2, \dots, \delta_k)$ such that $p' = \lambda q'$. Write

$$\lambda = \frac{f(\delta_2, \dots, \delta_k)}{g(\delta_2, \dots, \delta_k)},$$

where $f, g \in F[X_2, \dots, X_n]$, then $g(\delta_2, \dots, \delta_k)p' = f(\delta_2, \dots, \delta_k)q'$. Since $\delta_2, \dots, \delta_k$ are algebraically independent, this yields $g \cdot p = f \cdot q$. Since p is irreducible, it follows that $p|f$ or $p|q$. But f foes not depend on X_1 so $p|q$. Similarly $q|p$, and hence $p = \mu q\ (\mu \in F)$ and $r = k$. This proves the lemma. ∎

Note that we also have shown the following.

Lemma 1.1. *The polynomial associated with a circuit is essentially unique.* ∎

Next we discuss some preliminaries from matroid theory. Let (E, r) be a matroid (r is the rank function). A set $A \subseteq E$ is called a *double circuit* if $r(A)=|A|-2$ and $r(A-a)=|A-a|-1=|A|-2$ for each $a \in A$. (Compare this notion with circuits: a circuit is a set $A \subseteq E$ such that $r(A)=|A|-1$ and $r(A-a)=|A-a|=|A|-1$ for each $a \in A$.) Double circuits have a rather simple structure, as described by the following lemma.

Lemma 1.2. *If A is a double circuit in a matroid (E, r), then A has a partition $A = A_1 \cup \ldots \cup A_k$ such that $A - A_i$ is a circuit for $i=1, \ldots, k$, and these are all the circuits contained in A.*

Proof. Assume without loss of generality that $E=A$ and then consider the dual matroid. Clearly, this is a line without loops. Let $A_1, \ldots, A_k$ be the points of this line; then $\{A_1, \ldots, A_k\}$ is a partition of A. It also follows that $A_1, \ldots, A_k$ are the hyperplanes of the dual matroid, so $E-A_1, \ldots, E-A_k$ are the cocircuits of the dual matroid and hence they are the circuits of the original matroid. ∎

We call the number k of classes in the Lemma the *degree* of the double circuit. A double circuit of degree 2 is the direct sum of two circuits. In a graphic matroid, a double circuit of degree 3 corresponds to a Θ-graph. In a graphic (in fact, a binary) matroid, no double circuit has degree more then 3.

We need one more definition from matroid theory. Let (E, r) be a matroid, and $S \subseteq A \subseteq E$. We say that S is *in series in A* if contracting $A-S$, the set S becomes a circuit. Note that in this case, if a circuit in A contains one element of S, then it contains all.

We next prove the main theorem of this paper, which establishes those combinatorial properties of algebraic matroids which will be used in the sequel.

Theorem 1.3. The series reduction theorem. *Let $F \subseteq K$ be two algebraically closed fields and $S \subseteq A \subseteq K$ such that A is finite and S is in series in A in the matriod $\mathcal{A}(K/F)$. Then there exists a $\beta \in K$ such that for each $T \subseteq A-S$, the set $T \cup \{\beta\}$ is independent if and only if $T \cup S$ is independent, or, equivalently, $T \cup \{\beta\}$ is a circuit iff $T \cup S$ is a circuit.*

Proof. If S is a circuit then $\beta=0$ satisfies the requirements, so we may assume that this is not the case.

Let $F'=\mathrm{cl}_F(A-S)$. Then $\mathcal{A}(K/F')$ arises from $\mathcal{A}(K/F)$ by contracting the elements of $A-S$ (but leaving them there as loops). Hence S is a circuit in $\mathcal{A}(K/F')$ and so there is an irreducible polynomial $p \in F'[X_S]$ such that $p\|_{X_S=S}=0$. We may assume that at least one coefficient of p is 1. Let L denote the algebraically closed field generated by the coefficients of p.

Claim. *Let $T \subseteq A-S$. Then* $\mathrm{tr}_F(S \cup T) < \mathrm{tr}_F(T)+|S|$ *if and only if* $L \subseteq \mathrm{cl}_F(T)$.

Proof. For, assume first that $\mathrm{tr}_F(S \cup T) < \mathrm{tr}_F(T)+|S|$. Then S is dependent over $\mathrm{cl}_F(T)$, and hence there exists and irreducible polynomial $q \in \mathrm{cl}_F(T)[X_S]$ such that $q\|_{X_S=S}=0$. Now q remains irreducible over every extension field of $\mathrm{cl}_F(T)$, so in particular it is irreducible over F'. Hence by Lemma 1.1, $q=\lambda p$ for some $\lambda\in F'$. Considering the coefficient of p which is 1, we have $\lambda\in \mathrm{cl}_F(T)$ and hence $L\subseteq \mathrm{cl}_F(T)$.

Conversely, assume that $L\subseteq \mathrm{cl}_F(T)$. Then p shows that S is algebraically dependent over $\mathrm{cl}_F(T)$, and hence

$$\mathrm{tr}_{\mathrm{cl}_F(T)}(S) = r(S\cup T)-r(T) < |S|.$$

This proves the Claim. ∎

Now L is an infinite field and so it cannot be covered by finitely many proper subfields. So there exists a $\beta\in L$ which is not contained in any field $\mathrm{cl}_F(T)$ such that $L\nsubseteq \mathrm{cl}_F(T)$, i.e. such that $\mathrm{tr}_F(S\cup T)=\mathrm{tr}_F(T)+|S|$. For this β and any set $T\subseteq A-S$, $\beta\in \mathrm{cl}_F(T)$ if and only if $\mathrm{tr}_F(S\cup T)<\mathrm{tr}_F(T)+|S|$. So $T\cup S$ is independent if and only if $T\cup\{\beta\}$ is independent. ∎

Corollary 1.4. *Let $F\subseteq K$ be algebraically closed fields and let $A\subseteq K$ be a double circuit of degree k in $\mathscr{A}(K/F)$. Then*

$$\mathrm{tr}_F\big(\bigcap\{\mathrm{cl}_F(C)\colon\ C \text{ is a circuit in } A\}\big) \geqq k-2.$$

In particular, if $k\geqq 3$ then is an element $\delta\in K-F$ such that δ is contained in the algebraic closure of every circuit in A.

To get the Ingleton—Main Lemma from this theorem, choose two points from each of e_1, e_2 and e_3, to get a double circuit A. Then Theorem 1.3. says that there is an element $\delta\in K-F$ such that δ is contained in all three planes spanned by e_1 and e_2, e_1 and e_3 and e_2 and e_3, respectively. It is easy to see that δ is then contained in each of e_1, e_2 and e_3.

Proof of Corollary 1.4. Consider the partition $A=A_1\cup\ldots\cup A_k$ as in Lemma 1.2. We have $k\geqq 3$ by hypothesis. If $|A_i|=1$ for all $1\leqq i\leqq k$ then $\mathrm{cl}_F(C)\supseteq A$ for each circuit C in A and hence the assertion is obvious. Suppose that, say, $|A_1|\geqq 2$. Now A_1 is in series in A and hence by the Series Reduction Theorem, there is an element $\beta\in K$ such that for each $T\subseteq A-A_1$, the set $T\cup\{\beta\}$ is a circuit iff $T\cup A_1$ is a circuit. Hence $A'=(A-A_1)\cup\{\beta\}$ is also a double circuit of degree k. But then, by induction on $|A|$, we may assume that

$$\mathrm{tr}_F\big(\bigcap\{\mathrm{cl}_F(C')\colon\ C' \text{ is a circuit in } A'\}\big) \geqq k-2.$$

However, there is a bijection between circuit in A and circuits in A' such that if C is a circuit in A and C' is the corresponding circuit in A', then $\mathrm{cl}_F(C)\supseteq \mathrm{cl}_F(C')$. Hence

$$\mathrm{tr}_F\big(\bigcap\{\mathrm{cl}_F(C)\colon\ C \text{ is a circuit in } A\}\big) \geqq k-2. \ ∎$$

We have mentioned that the rank function of a full algebraic matroid is not in general modular of the flats (algebraically closed subfields). Hence the intersection $U\cap V$ of two flats U and V looses some of the properties it enjoys in full linear matroids. The following result shows that a certain "quasi-intersection" can be defined which simulates $U\cap V$ in a sense.

Theorem 1.5. *Let $\mathscr{A}(K/F)$ be a full algebraic matroid of finite rank and U and V, two flats in $\mathscr{A}(K/F)$. Then there exists a flat $T=T(U,V)\subseteq U$ such that for each flat*

$W \subseteq U$, we have $T \subseteq W$ if and only if

$$r(W \cup V) - r(W) = r(U \cup V) - r(U).$$

Remark. Note that in general $T(U, V) \nsubseteq V$. In fact, $T(U, V) \subseteq V$ if and only if the rank function is modular on the pair U, V, in which case $T(U, V) = U \cap V$. The property of T stated in the theorem is also equivalent to the following: for each flat $W \subseteq U$,

$$r(V \cup W) - r(V) = r(V \cup T \cup W) - r(V \cup T).$$

Proof. Let B be any basis of V, and let $C_1, \ldots, C_m$ be the circuits of $\mathscr{A}(K/U)$ contained in B. For each C_i, let $p_i \in U[X_{C_i}]$ be an irreducible polynomial such that $p_i\|_{X_{C_i}=C_i} = 0$. Also assume that p_i has at least one coefficient which is equal to 1. Let $T(U, V)$ be the algebraically closed field generated by the coefficients of $p_i, \ldots, p_m$. The proof that this choice of $T(U, V)$ satisfies the requirements in the theorem is a straightforward extension of the proof of the Claim in Theorem 1.3. ∎

If we have any matroid in which

(i) no flat is the union of finitely many proper subflats;

(ii) the assertion of Theorem 1.5 holds,

then also the series reduction theorem holds.

2. Matroid matching and fullness of matroids

Let (E, r) be a matroid and let $\mathscr{H}$ be any family of lines in (E, r). We shall write, for brevity, $r(\mathscr{H})$ instead of $r(\bigcup \mathscr{H})$. We say that $\mathscr{H}$ is a *matching of lines* if $r(\mathscr{H}) = 2|\mathscr{H}|$. We say that $\mathscr{H}$ is a *circuit of lines* if $r(\mathscr{H}) = 2|\mathscr{H}| - 1$ but $r(\mathscr{H} - e) = 2|\mathscr{H} - e|$ for every $e \in \mathscr{H}$. We say that $\mathscr{H}$ is a *double circuit of lines* if $r(\mathscr{H}) = 2|\mathscr{H}| - 2$ but $r(\mathscr{H} - e) = 2|\mathscr{H} - e| - 1$ for every $e \in \mathscr{H}$.

Two coplanar lines form a circuit of lines. Three lines which are not coplanar but any two of which are coplanar form a double circuit of lines.

If $\mathscr{H}$ is a matching and we choose two independent elements from each line in $\mathscr{H}$, then the elements chosen are independent in the matroid. If $\mathscr{H}$ is a circuit of lines, and we choose two independent elements from each line in $\mathscr{H}$, then the elements chosen form a set H with $r(H) = |H| - 1$. (If $\mathscr{H}$ consists of two lines intersecting in a point and the common point is chosen from both lines then we assume that this element occurs with multiplicity larger than one, and that different elements of the intersection point of the two lines are chosen as representatives). Hence H contains a unique circuit C. It is clear that C contains at least one point from each of the lines.

If $\mathscr{H}$ is a double circuit of lines, and we choose two independent elements from each line in $\mathscr{H}$, then the set H of elements chosen satisfies $r(H) = 2|H| - 2$. Hence in contains a unique double circuit A. Let $A = A_1 \cup \ldots \cup A_k$ be the canonical partition of this double circuit. It is easy to see that each line in $\mathscr{H}$ contains at least one point from A, but if it contains two then these belong to the same class A_i. Hence $\mathscr{H}_i = \{e \in \mathscr{H} : e \cap A_i \neq \emptyset\}$ defines a partition $\mathscr{H} = \mathscr{H}_1 \cup \ldots \cup \mathscr{H}_k$ of $\mathscr{H}$. The sets $\mathscr{H} - \mathscr{H}_i$ are circuits of lines. We call $\mathscr{H}$ *trivial* if $k = 2$ and *nontrivial* if $k \geqq 3$.

The *matroid matching problem* is the following: given a family $\mathscr{H}$ of lines in a matroid (E, r), find a maximum cardinality subfamily which forms a matching. In (Lovász [5]) the following was proved: if $\nu(\mathscr{H})$ denotes the maximum cardinality of a matching in $\mathscr{H}$, if $A \subseteq E$ is any flat in (E, r) and $\{\mathscr{H}_1, \ldots, \mathscr{H}_k\}$ is any partition of $\mathscr{H}$, then

$$(*) \qquad \nu(\mathscr{H}) \leqq r(A) + \sum_{i=1}^{k} \left\lfloor \frac{r(\bigcup \mathscr{H}_i \cup A) - r(A)}{2} \right\rfloor.$$

Let $\bar{\nu}(\mathscr{H})$ denote the minimum of the right hand side here, taken over all flats A and all partitions $\{\mathscr{H}_1, \ldots, \mathscr{H}_k\}$ of $\mathscr{H}$. We do not always have $\bar{\nu}(\mathscr{H}) = \nu(\mathscr{H})$; for example, let $\mathscr{H}$ consist of all lines in an affine space parallel to a given line. But if we embed the affine space into a projective space by adding elements at infinity, then the choice $A = \{$common point at infinity of the given lines$\}$ and $\{\mathscr{H}_1, \ldots, \mathscr{H}_k\} = \{$partition of $\mathscr{H}$ into singletons$\}$ gives equality in $(*)$. We do not know whether every matroid can be embedded into one in which $\nu(\mathscr{H}) = \bar{\nu}(\mathscr{H})$ for a given family $\mathscr{H}$ of lines in the original matroid.

In [5] it was proved that $\nu(\mathscr{H}) = \bar{\nu}(\mathscr{H})$ holds for any family of lines in a projective space. The somewhat more transparent proof in [6] in fact shows more:

Theorem 2.1. *If for every contraction (E, r') of (E, r), and for every non-trivial double circuit $\mathscr{D}$ of lines in (E', r') there is a point $p \in E'$ which is contained in the closure of every circuit $\mathscr{C} \subseteq \mathscr{D}$, then $\nu(\mathscr{H}) = \bar{\nu}(\mathscr{H})$ for every collection $\mathscr{H}$ of lines in (E, r).* ▮

We have mentioned several properties of matroids which all are connected to "fullness" in some sense. Let us introduce them formally.

Let us say that a matroid (E, r) has the *series reduction property* if for all $S \subseteq A \subseteq E$ such that A is finite and S is in series in A, there is an element $\beta \in E$ such that for each $T \subseteq A - S$, the set $T \cup S$ is a circuit iff $T \cup \{\beta\}$ is a circuit. We shall also need weaker versions of this property: we say that (E, r) has the *weak series reduction property* if the above holds for all $S \subseteq A \subseteq E$ such that in addition $A - S$ induces a connected matroid. We have proved that full algebraic matroids have the series reduction property. The polygon matroid of a complete graph, with all edges with infinite multiplicity, on the other hand, has the weak series reduction property but not the stronger one. In fact, if S consists of two edges which form a cut in A but are not consecutive, then no β with the desired properties exists. (We shall call the polygon matroid of a complete graph with all edges with infinite multiplicity a *full graphic matroid.*)

The linear independence matroid of a linear space over a skew field, which we call a *full linear matroid,* also has the series reduction property, even in the stronger sense. This follows easily from the fact that its flat lattice is modular.

We mention one more matroid with the weak series reduction property. Let V be a finite set and let E consists of infinitely many copies of each subset of V. Define a matroid on E by letting a set $X \subseteq E$ be independent iff X has a system of distinct representatives. Note that this is a transversal matroid; we have, however, interchanged "sets" and "elements" relative to the usual definition. We call the resulting matroid (E, r) the *full transversal matroid* of rank $|S|$.

Lemma 2.2. *Every full transversal matroid has the weak series reduction property.*

Proof. Let us remark first that the rank function of a transversal matroid as defined above is given by the well-known formula

$$(1)\qquad r(A) = \min_{X \subseteq A} \{|\cup X| + |A - X|\}.$$

If A has no coloop, i.e. if $r(A-x)=r(A)$ for all $x \in A$ then we in fact have

$$(2)\qquad r(A) = |\cup A|;$$

for, if X is the set providing the minimum in (1) and $X \neq A$ then for any $x \in A - X$ we have

$$r(A-x) \leqq |\cup X| + |A-x-X| = r(A)-1,$$

i.e. x is a coloop of A.

Now let $S \subseteq A \subseteq E$, S in series in A and $A-S$ connected. Then by (2),

$$|\cup A| = r(A)$$

and

$$|\cup (A-S)| = r(A-S).$$

Since S is in series in A, we have

$$|S|-1 = r(A)-r(A-S) = |\cup A| - |\cup (A-S)| = |\cup S - \cup (A-S)|.$$

Let $\beta \in (\cup (A-S)) \cap (\cup S)$. We claim that β satisfies the requirements of the series reduction property. For, let $T \subseteq A-S$ and assume that $T \cup S$ is a circuit. Then by (2) again,

$$|\cup (T \cup S)| = r(T \cup S) = |T \cup S| - 1.$$

On the other hand,

$$|\cup (T \cup S)| \geqq |\cup S - \beta| + |\cup T| \geqq |S| - 1 + |T| = |T \cup S| - 1.$$

Hence $|\cup T| = |T|$ and $\beta \in \cup T$. So $|\cup (T \cup \{\beta\})| = |\cup T| = |T| = |T \cup \{\beta\}| - 1$, i.e. $T \cup \{\beta\}$ is dependent. On the other hand, if $T' \subset T$ then $S \cup T'$ is independent and hence $|\cup (S \cup T')| \geqq |S| + |T'|$. But we have

$$|\cup (S \cup T')| \leqq |\cup S - \beta| + |(\cup T') \cup \beta| = |S| - 1 + |(\cup T') \cup \beta|$$

and so

$$|(\cup T') \cup \beta| \geqq |T'| + 1 = |T' \cup \{\beta\}|.$$

This proves that $T \cup \{\beta\}$ is a circuit.

The converse implication follows by the same argument as used in the proof of Theorem 1.3. ∎

Let us say that a matroid (E, r) has the *double circuit property* if for every double circuit $A \subseteq E$ of degree k, there are $k-2$ independent points $p_1, \ldots, p_{k-2}$ in E contained in the closure of each circuit in A.

We say that (E, r) has the *matching property* if $\nu(\mathcal{H}) = \bar{\nu}(\mathcal{H})$ holds for every collection $\mathcal{H}$ of lines in (E, r).

Lemma 2.3. *The weak and strong series reduction properties, and the double circuit property are preserved under contraction.* ▮

The proof is routine and is omitted.

Then we can easily prove the following theorem.

Theorem 2.4.

(a) If a matroid has the weak series reduction property, then it has the double circuit property.

(b) If a matroid has the double circuit property, then it has the matching property.

Proof. *(a)*. This follows by the same proof as Corollary 1.4.

(b) It suffices to show, by Theorem 2.1, that if $\mathscr{D}$ is any non-trivial double circuit of lines in a matroid (E, r) with the double cirucit property, then there exists an element contained in the closure of every circuit of lines in $\mathscr{H}$. Let us choose two independent elements from each line in $\mathscr{D}$ and let A be the unique double circuit contained in the set of elements chosen. Since $\mathscr{D}$ is non-trivial, A has degree $k \geqq 3$ and hence by the double circuit property, there is a point p in (E, r) contained in the closure of each circuit in A. But the closure of each circuit in $\mathscr{D}$ contains a circuit in A and hence also contains p. ▮

Corollary 2.5. *Full algebraic matroids, full linear matroids, full graphic matroids and full transversal matroids have the matching property.* ▮

Let us remark that the fact that the matroid matching problem can be solved easier for graphic and transversal matroids was noted earlier (Lovász [6], Po Tong, Lawler and Vazirani [8]). Both of these classes are of course representable over, say, the rational field as linear matroids. This means that they can be embedded in a full linear matroid, which has the matching property and hence a min—max formula for the maximum size of a matching can be derived. This, however, involves a linear subspace ranging through all linear subspaces of the full linear matroid. The preceding corollary says that we may restrict ourselves to subspaces of the full graphic and transversal matroid, respectively.

We conclude with couching the matroid matching theorem for algebraic matroids in a more algebraic form.

Corollary 2.6. *Let $F \subseteq K$ be two fields and let $\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n$ be elements in K such that $\mathrm{tr}_F\{\alpha_i, \beta_i\} = 2$ for all i. Then the maximum number of pairs (α_i, β_i) whose union is algebraically independent over F is given by the minimum of the expression*

$$\mathrm{tr}_F(F') + \sum_{j=1}^{k} \left\lfloor \frac{1}{2} \mathrm{tr}_{F'}\left(\cup\{\{\alpha_i, \beta_i\} \colon i \in I_j\}\right) \right\rfloor$$

where F' ranges over all extensions of F in K and $\{I_1, \ldots, I_k\}$, over all partitions of $\{1, \ldots, n\}$. ▮

References

[1] A. W. INGLETON and R. A. MAIN, Non-algebraic matroids exist. *Bull. Lonbon Math. Soc.* **7** (1975) 144—146.
[2] P. M. JENSEN and B. KORTE, Complexity of matroid property algorithms. *SIAM J. on Computing*, **11** (1982) 184—190.
[3] B. LINDSTRÖM, A non-algebraic matroid of rank three. *Math. Scandinavica (submitted).*
[4] B. LINDSTRÖM, On harmonic conjugates in algebraic matroids. *Europ. J. Comb. (submitted).*
[5] L. LOVÁSZ, Selecting independent lines from a family of lines in a projective space. *Acta Sci. Math.* **42** (1980), 121—131.
[6] L. LOVÁSZ, Matroid matching and some applications. *J. Comb. Theory* **28** (1980), 208—236.
[7] L. LOVÁSZ, The matroid matching problem. *in: Algebraic Methods in Graph Theory, Coll. Math Soc. J. Bolyai* **25**, North Holland, Amsterdam 1981.
[8] PO TONG, E. L. LAWLER and V. V. VAZIRANI, Solving the Weighted Parity problem for gammoids by reduction to graphic matching. *in: Progress in Combinatorial Optimization* (W. Pulleyblank, ed.), Academic Press, 1984, 363—374.
[9] VAN DER WAERDEN, *Moderne Algebra.* 2nd edition, Berlin, 1937, 6th edition, Springer, Berlin/Heidelberg/New York, 1967.

A. Dress

Fakultät f. Math.
Universität Bielefeld
D-4800 Bielefeld 1
G.F.R.

L. Lovász

Dept. Comp. Sci.
Mathematical Institute
Eötvös University
1088, Múzeum krt 6—8.
Hungary