MATH. SCAND. 63 (1988), 36–42

ON P-POLYNOMIAL REPRESENTATIONS OF PROJECTIVE GEOMETRIES IN ALGEBRAIC COMBINATORIAL GEOMETRIES

BERNT LINDSTRÖM

Abstract.

A p-polynomial in the ring $F[X_1,\ldots,X_n]$ over a field F of prime characteristic p is a linear combination of terms $X_i^{p^h}$, $1 \leqq i \leqq n$, $h \geqq 0$. These p-polynomials represent points in the full algebraic combinatorial geometry of $F(X_1,\ldots,X_n)$. The full algebraic combinatorial geometry is not a projective geometry, it is only semimodular, but the p-polynomial points give a projective subgeometry (Theorem 2). The subgeometry can be coordinatized by a skew-field, which is quotient ring of an Ore-domain (Theorem 1). Elements in the Ore-domain are all p-polynomials in $F[X]$.

If $F \neq \mathrm{GF}(p)$, then the coordinatizing skew-field is noncommutative and it follows that Pappus' theorem does not hold in the geometry. This implies the existence of algebraic representations over fields of prime characteristic of the non-Pappus matroid found before by the author by trial and error. Algebraic representations of the dual matroid were not known before.

1. Introduction.

We will assume some familiarity with projective geometries over division rings (see [1]) and elementary theory of matroids and combinatorial geometries (see [2] and [9]).

Algebraic combinatorial geometries and matroids are more general than linear combinatorial geometries and matroids over a field F. The former are defined in terms of algebraic dependence over F. The latter are defined in terms of linear dependence over F. There is a simple transformation from linear representations to algebraic representations which replaces a vector $(a_1,\ldots,a_n)$ with components in F with a number $a_1x_1+\ldots+a_nx_n \in F(x_1,\ldots,x_n)$, where $x_1,\ldots,x_n$ are algebraically independent transcendentals over F (see [9, Theorem 11.2.1]).

Algebraic representations of simple matroids can be embedded in *full algebraic combinatorial geometries*. These are combinatorial geometries the

Research supported by the Swedish Natural Science Research Council.

Received July 04, 1986; in revised form October 10, 1986.

points of which are algebraically closed fields $\overline{F(x)}$ of transcendence degree 1 over F, lines are algebraically closed fields $\overline{F(x,y)}$ of transcendence degree 2 over F, planes are algebraically closed fields $\overline{F(x,y,z)}$ of transcendence degree 3 over F etc. These combinatorial geometrics contain the classical projective geometries over F if we identify a point $(a_1,\dots,a_n)$ in the projective geometry with the point $\overline{F(a_1x_1+\dots+a_nx_n)}$ in the full algebraic combinatorial geometry. The latter have many properties in common with projective geometries; e.g. one can prove that the converse of Desargues' theorem holds (see [6]). But they are not projective geometries for the modularity fails (two lines in a plane do not always meet in a point).

It is amusing to see that these full algebraic combinatorial geometries contain copies of the projective spaces over the rational field Q even when the characteristic of F is a prime: identify the point $(a_1,\dots,a_n)$ with components in Q with the field $\overline{F(a_1^{a_1}\dots x_n^{a_n})}$. Recall that $(a_1,\dots,a_n)$ and $(ka_1,\dots,ka_n)$, with $k \neq 0$, represent the same point. Therefore we may assume that $a_1,\dots,a_n$ are integers. It is an easy exercise to prove that linear independence of vectors $(a_1,\dots,a_n) \neq (0,\dots,0)$ over Q corresponds to algebraic independence of the monomials $x_1^{a_1}\dots x_n^{a_n}$ over F, where F is any field.

More interesting is that full algebraic combinatorial geometries contain projective geometries which are strictly larger than the classical ones; when the characteristics of F is a prime p; this is the main result of the present paper. We call these algebraic projective geometries p-polynomial.

A *p-polynomial* is a polynomial in the ring $F[X_1,\dots,X_n]$ which is a linear combination of terms $X_i^{p^h}$, $1 \leqq i \leqq n$, $h \geqq 0$ (p is the characteristic of F). We borrow this notion from the theory of linear algebraic groups (see [4, p. 129]). The points $\overline{F(P)}$, where $P \neq 0$ is a p-polynomial, will give the p-polynomial algebraic projective geometry. Note that the previous points $\overline{F(a_1x_1+\dots+a_nx_n)}$ of the projective geometry over F are among them.

We now recall that projective geometries other than the classical ones are obtained by using vectors with components in a skew-field. By a famous result of Hilbert in "Grundlagen der Geometrie" Pappus' theorem holds if and only if the coordinatizing skew-field is a field. We shall prove that our p-polynomial projective geometries can be coordinatized by skew-fields, which are noncommutative when $F \neq \mathrm{GF}(p)$. It follows that the non-Pappus matroid, which violates Pappus' theorem, has p-polynomial algebraic representation over F when $F \neq \mathrm{GF}(p)$. Explicit representations over $\mathrm{GF}(p^2)$ were found by the author [7]. We should mention that there are algebraic representations over $\mathrm{GF}(p)$ which are not p-polynomial (see [5]).

I will now describe the coordinatizing skew-fields in our p-polynomial algebraic projective geometries. Let F be a field of characteristic p and $\boldsymbol{R}$ the set of all p-polynomials in $F[X]$. Each polynomial is a linear combination of terms X^{p^h}, $h \geqq 0$, with coefficeints in F. We now define two operations $+$ and $\cdot$ in $\boldsymbol{R}$ which will make $\boldsymbol{R}$ a ring. The sum of $P(X)$ and $Q(X) \in \boldsymbol{R}$ is the ordinary sum of polynomials $P(X)+Q(X)$. The product of $P(X)$ and $Q(X)$ is the composition $P(Q(X))$. We leave the verification of the usual ring axioms for the reader. Note that the distributive law

$$P(Q_1(x)+Q_2(X)) = P(Q_1(X))+P(Q_2(X))$$

depends on $(a+b)^{p^m} = a^{p^m}+b^{p^m}$ valid in characteristic p. Note that $\boldsymbol{R}$ is a ring without zero divisors: $P(Q(X)) = 0$ implies that $P(X) = 0$ or $Q(X) = 0$. If we choose $P(X) = \lambda X$ with $\lambda \in F$ and $Q(X) = X^p$, then $P(Q(X)) = \lambda X^p$ and $Q(P(X)) = \lambda^p X^p$. If $F \neq \mathrm{GF}(p)$, we can determine λ such that $\lambda^p \neq \lambda$, and $\boldsymbol{R}$ will be noncommutative.

For any two nonzero p-polynomials $P(X)$ and $Q(X)$ there are nonzero p-polynomials $R(X)$ and $S(X)$ such that $R(P(X)) = S(Q(X))$ (Lemma 1). This is a *left Ore-condition*. The ring $\boldsymbol{R}$ is therefore an *Ore-domain*. By a result of Ore in [8] the ring can be embedded in a skew-field. (Ores construction of the skew-field depends on a right Ore-condition.) We will apply the presentation in [3, p. 170]. Each element of the skew-field is an equivalence class class of pairs (P, Q) of elements in the ring with $Q \neq 0$. Two pairs (P_i, Q_i), $i = 1, 2$, are equivalent if $RQ_1 = SQ_2$ implies $RP_1 = SP_2$, R, $S \in \boldsymbol{R}$. The sum

$$(P_1, Q_1)+(P_2, Q_2) = (RP_1+SP_2, RQ_1),$$

where $RQ_1 = SQ_2$, $R, S \neq 0$. Multiplication is defined by

$$(P_1, Q_1)(P_2, Q_2) = (TP_2, UQ_1),$$

where $TQ_2 = UP_1$, $U \neq 0$. We write here for brevity P_i in place of $P_i(X)$, and RQ_1 in place of $R(Q_1(X))$. The skew-field is denoted by $Q(\boldsymbol{R})$ as in [3, p. 170]. Note that $Q(\boldsymbol{R})$ contains an isomorphic copy of $\boldsymbol{R}$: we may identify $P(X)$ in $\boldsymbol{R}$ with $(P(X), X)$ in $Q(\boldsymbol{R})$.

For later use we now prove that each point in a projective geometry of rank n over $Q(\boldsymbol{R})$ can be represented by an n-tuple of elements of $\boldsymbol{R}$, i.e. p-polynomials. Let $(a_1, \ldots, a_n)$ be a nonzero n-tuple of elements in $Q(\boldsymbol{R})$. Assume that $a_i = (P_i, Q_i)$, $Q_i \neq 0$, for $i = 1, \ldots, n$. By a straightforward generalization of the left Ore-condition using induction over $i = 1, \ldots, n$ follows the existence of nonzero p-polynomials $R_i(X) \in F[X]$ such that $R_i(Q_i)$ does not depend on i. Let

$$c = (R_i(Q_i(X)), X) \in Q(\boldsymbol{R}).$$

Then we find $ca_i = (R_i(P_i(X)), X)$ by the definition of multiplication in $Q(\boldsymbol{R})$. Hence, we may identify ca_i with the p-polynomial $R_i(P_i(X))$. But $(ca_1, \ldots, ca_n)$ and $(a_1, \ldots a_n)$ represent the same point in the projective geometry over

$Q(\boldsymbol{R})$. Therefore we may use n-tuples of p-polynomials to represent points in the projective geometry. This is analogous to the representation of points in a projective space over the rational numbers by n-tuples of integers.

2. Main results.

We prove first

THEOREM. 1. *Let F be a field of characteristic $p > 0$. The set of p-polynomials in $F[X]$ is an Ore-domain when the sum of two elements $P(X)$ and $Q(X)$ is the usual sum $P(X)+Q(X)$ and product is the composition $P(Q(X))$.*

After the discussion given in the introduction it remains to prove:

LEMMA 1. *$P(X)$ and $Q(X) \in F[X]$ be nonzero p-polynomials. Then there are nonzero p-polynomials $R(X)$ and $S(X) \in F[X]$ such that $R(P(X)) = S(Q(X))$.*

PROOF. The proof is by induction over $\deg P + \deg Q = n \geqq 2$. If $n = 2$, then $\deg P = \deg Q = 1$, and we may find $R(X)$ and $S(X)$ of degree 1. Assume that $n > 2$ and let $\deg P \geqq \deg Q$. Then we can find $m \geqq 0$ such that $\deg P^{p^m} = \deg Q$ and $a \in F$ such that either $P^{p^m} = aQ$ or $\deg(P^{p^m} - aQ) < \deg Q$.

In the first case define $R'(X) = X^{p^m}$ and $S'(X) = aX$. In the second case there are nonzero p-polynomials $R(X)$ and $S(X) \in F[X]$ such that $R(P^{p^m} - aQ) = S(Q)$ by the induction hypothesis. Let

$$R'(X) = R(X^{p^m}) \quad \text{and} \quad S'(X) = S(X) - R(-aX).$$

In both cases we have $R'(P) = S'(Q)$, which was to be proved.

THEOREM 2. *Let F be a field of prime characteristic p. The p-polynomials in $F[X_1, \ldots, X_n]$ then represent all points of a modular algebraic subgeometry of the full algebraic combinatorial geometry of $F(X_1, \ldots, X_n)$. This subgeometry is as projective geometry over the quotient skew-field $Q(\boldsymbol{R})$ of the Ore-domain $\boldsymbol{R}$ in Theorem 1. The subgeometry is Pappian if and only if $F = \mathrm{GF}(p)$.*

The proof will depend on the following lemma.

LEMMA 2. *Let $P_1, \ldots, P_m$ $(m \geqq 2)$ be nonzero p-polynomials in $F[X_1, \ldots, X_n]$. Then $P_1, \ldots, P_m$ are algebraically dependent over F if and only if there are p-polynomials $Q_1, \ldots, Q_m \in F[X]$, not all 0, such that $Q_1(P_1) + \ldots + Q_m(P_m) = 0$.*

PROOF. Write $P_i = P_{i1}(X_1) + \ldots + P_{in}(X_n)$ for $i = 1, \ldots, m$, where $P_{ij}(X_j)$ is a p-polynomial in $F[X_j]$. The existence of the p-polynomials

$$Q_1(X), \ldots, Q_m(X) \in F[X]$$

will be proved by induction over $n \geqq 1$. When $n = 1$ the result follows by Lemma 1.

Let $n \geqq 2$. Assume that the lemma is true for $n-1$ indeterminates. We may assume without loss of generality that $P_{11}(X_1) \neq 0$.

Assume that $P_{i1} \neq 0$ for some $i \in \{2,\ldots,m\}$. By Lemma 1, there are p-polynomials $R_i(X)$ and $S_i(X)$ in $F[X]$ with $R_i, S_i \neq 0$ such that $R_i(P_{i1}) = S_i(P_{11})$.

For $j \in \{2,\ldots,m\}$ such that $P_{i1} = 0$ define $R_j(X) = X$ and $S_j(X) = 0$.

It follows that $R_j(P_j) - S_j(P_1)$ does not depend on X_1 when $j = 2,\ldots,m$. Note that $R_j \neq 0$ for $j = 2,\ldots,m$.

Let $\boldsymbol{R}$ be the Ore-domain of all p-polynomials $P(X)$ in $F[X]$, and let $Q(\boldsymbol{R})$ be the corresponding skew-field (cf. the Introduction).

If $R_j(P_j) - S_j(P_1) = 0$ for any $j \in \{2,\ldots,m\}$ we are finished. Therefore we may assume that $R_j(P_j) - S_j(P_j) \neq 0$ for $j = 2,\ldots,m$. We claim that these polynomials in $F[X_2,\ldots,X_n]$ are algebraically dependent over F.

Assume that they are algebraically independent over F. It follows

$$m = \text{tr.d.}_F F(P_1, R_2(P_2)-S_2(P_1),\ldots, R_m(P_m)-S_m(P_1)) \\ \leqq \text{tr.d.}_F F(P_1,\ldots,P_m) < m,$$

since $P_1,\ldots,P_m$ are algebraically dependent over F by assumption. The contradiction proves tht the polynomials $R_j(P_j) - S_j(P_1)$, $j = 2,\ldots,m$, are algebraically dependent over F.

By the induction hypothesis, there are p-polynomials $T_2,\ldots,T_m$ in $F[X]$, not all 0, such that

$$T_2(R_2(P_2)-S_2(P_1))+\ldots+T_m(R_m(P_m)-S_m(P_1)) = 0.$$

We may rewrite this relation

$$T_2(R_2(P_2))+\ldots+T_m(R_m(P_m))+V(P_1) = 0,$$

where $V(X) \in F[X]$ is a p-polynomial. Since $R_2,\ldots,R_m$ are nonzero polynomials in $F[X]$ and at least one of $T_2,\ldots,T_m$ is nonzero, it follows that at least one of the p-polynomials $T_2(R_2(\mathrm{X})),\ldots,T_m(R_m(X))$ is nonzero. This completes the proof of the "only if" part of the lemma. The implication in the other direction follows by the definition of algebraic dependence.

Proof of Theorem 2. Define a bijection f from the set of all n-dimensional vectors with p-polynomial components in $F[X]$ onto the set of all p-polynomials in $F[X_1,\ldots,X_n]$ by

$$f((P_1(X),\ldots,P_n(X)) = P_1(X_1)+\ldots+P_n(X_n).$$

Recall that all points in a rank n-projective geometry over $Q(\boldsymbol{R})$ are represented by p-polynomial vectors $(P_1(X),\ldots,P_n(X)) \neq (0,\ldots,0)$.

If $(P_1(X),\ldots,P_n(X))$ and $(Q_1(X),\ldots,Q_n(X))$ represent the same point in the projective geometry, it is easy to see that there are nonzero p-polynomials $R(X)$ and $S(X)$ in $F[X]$ such that $R(P_i(X)) = S(Q_i(X))$ for $i = 1,\ldots,n$. Let

$$f((P_1(X),\ldots,P_n(X)) = P \quad \text{and} \quad f((Q_1(X),\ldots,Q_n(X)) = Q.$$

Then we have $R(P) = S(Q)$, i.e. P and Q are algebraically dependent over F. It follows that f induces a map $\bar{f}$ from the set of all points in the projective geometry over $\underline{Q(\boldsymbol{R})\text{ into }}$ the set of points of the algebraic combinatorial geometry of $\overline{F(X_1,\ldots,X_n)}$. It follows by Lemma 2 ($m = 2$) that the map $\bar{f}$ is an injection.

More generally, it follows by Lemma 2 that linearly dependent sets of points in the projective geometry are mapped on algebraically dependent sets of points in the combinatorial geometry, and similarly for independent sets of points. Therefore there will be a one-one map between all flats (submanifolds) in the projective geometry and some of the flats in the combinatorial geometry, which preserves incidences between flats (isomorphic geometries give isomorphic geometric lattices).

A projective geometry is Pappian if and only if the coordinatizing skew-field in a field (see [1, p. 71]). It is easy to verify commutativity when $F = \mathrm{GF}(p)$. The Ore-domain $\boldsymbol{R}$ is noncommutative, when there exists $\lambda \in F$ with $\lambda^p \neq \lambda$, and this is the case when $F \neq \mathrm{GF}(p)$ (choose $P(X) = \lambda X$ and $Q(X) = X^p$).

This completes the proof of the theorem.

Corollary. *There are p-polynomial algebraic representations of the non-Pappus matroid M and its dual M* over F, when* $F \neq \mathrm{GF}(p)$.

Proof. The existence of p-polynomial representations of the non-Pappus matroid M over F follows immediately from the theorem.

We now define left and right representations over skew-field $\boldsymbol{S}$.

Multiplication on the left (right) of vectors over $\boldsymbol{S}$ gives a left (respectively right) projective geometry over $\boldsymbol{S}$. Corresponding representations of a matroid are called *left* (respectively *right*) *representations* of the matroid over $\boldsymbol{S}$.

We need the following generalization of [9, Theorem 9.3.2].

Lemma 3. *If a matroid M has a right representation over a skew-field* $\boldsymbol{S}$, *then its dual M* has a left representation over* $\boldsymbol{S}$.

An easy proof can be modelled on the proof of [9, Theorem 9.3.2] using the rank formula for adjoint spaces in [1, p. 33]. We leave the details for the reader.

Since the skew-field $Q(\boldsymbol{R})$ is noncommutative, there is a right representation of the non-Pappus matroid M over $Q(\boldsymbol{R})$. Then there is a left representation of M^* over $Q(\boldsymbol{R})$ by Lemma 3. Hence there is a p-polynomial algebraic representation of M^* over F.

REFERENCES

1. R. Baer, *Linear Algebra and Projective Geometry* (Pure and Appl. Math. 2), Academic Press, New York, 1952.
2. H. Crapo and G.-C. Rota, *Combinatorial Geometries*, M.I.T. Press, Cambridge, Mass., 1970.
3. I. N. Herstein, *Noncommutative Rings* (Carus Math. Monographs 15), John Wiley and Sons, Ltd., New York, London, 1968.
4. J. E. Humphreys, *Linear Algebraic Groups* (Graduate Texts in Math. 21), Springer-Verlag, Berlin - Heidelberg - New York, 1975.
5. B. Lindström, *The non-Pappus matroid is algebraic*, Ars Combin. 16 B (1983), 95–96.
6. B. Lindström, *A Desarguesian theorem for algebraic combinatorial geometries*, Combinatorica 5 (1985), 237–239.
7. B. Lindström, *The non-Pappus matroid is algebraic over any finite field*, Utilitas Math. 30 (1986), 53–55.
8. O. Ore, *Linear equations in noncommutative fields*, Ann. of Math. (2) 32 (1931), 463–477.
9. D. J. A. Welsh, *Matroid Theory* (London Math. Soc. Monographs 8), Academic Press, London, New York, San Francisco, 1976.

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