ANDRZEJ SCHINZEL

On a decomposition of polynomials in several variables

Journal de Théorie des Nombres de Bordeaux, tome 14, n° 2 (2002), p. 647-666

<http://www.numdam.org/item?id=JTNB_2002__14_2_647_0>

Journal de Théorie des Nombres de Bordeaux **14** (2002), 647–666

On a decomposition of polynomials in several variables

par ANDRZEJ SCHINZEL

Dedicated to Michel Mendès France

RÉSUMÉ. On considère la représentation d'un polynôme à plusieurs variables comme une somme de polynômes à une variable en combinaisons linéaires des variables.

ABSTRACT. One considers representation of a polynomial in several variables as the sum of values of univariate polynomials taken at linear combinations of the variables.

K. Oskolkov has called my attention to the following theorem used in the theory of polynomial approximation (see [6], Lemma 1 and below, Lemma 4): for every sequence of $d+1$ pairwise linearly independent vectors $[\alpha_{\mu 1}, \alpha_{\mu 2}] \in \mathbb{R}^2$ $(1 \le \mu \le d+1)$ and every polynomial $F \in \mathbb{C}[x_1, x_2]$ of degree d there exist polynomials $f_\mu \in \mathbb{C}[z]$ $(1 \le \mu \le d+1)$ such that

$$F = \sum_{\mu=1}^{d+1} f_\mu (\alpha_{\mu 1} x_1 + \alpha_{\mu 2} x_2) .$$

He has asked for a generalization and a refinement of this result. The following theorem is a step in this direction.

Theorem 1. *Let n, d be positive integers and K a field with* $\operatorname{char} K = 0$ *or* $\operatorname{char} K > d$. *For every sequence $S_\nu\,(2 \le \nu \le n)$ of subsets of K each of cardinality at least $d+1$ there exist $M = \binom{n+d-1}{n-1}$ vectors $[\alpha_{\mu 1}, \alpha_{\mu 2}, \dots, \alpha_{\mu n}] \in \{1\} \times S_2 \times \dots \times S_n$ with the following property. For every polynomial $F \in K[x_1, \dots, x_n]$ of degree at most d there exist polynomials $f_\mu \in K[z]$ $(1 \le \mu \le M)$ such that*

$$F = \sum_{\mu=1}^{M} f_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu \right) . \tag{1}$$

Manuscrit reçu le 2 mars 2001.

It is not true that polynomials f_μ satisfying (1) exist for every sequence of vectors $[\alpha_{\mu 1}, \dots, \alpha_{\mu n}]$ $(1 \le \mu \le M)$ such that each n of them are linearly independent. See the example at the end of the paper.

Let $P(n,d,K)$ be the set of all polynomials $F \in K[x_1, \dots, x_n]$ of degree d. Let $M(n,d,K)$ be the least number M such that for every $F \in P(n,d,K)$ (1) holds for some sequence of vectors $[\alpha_{\mu 1}, \dots, \alpha_{\mu n}] \in K^n$ and some sequence of polynomials $f_\mu \in K[z]$ $(1 \le \mu \le M)$ if such sequences exist and ∞ otherwise. For an infinite field K, let $m(n,d,K)$ be the least number M such that for a Zariski open subset S of $P(n,d,K)$ and for every $F \in S$, (1) holds for some sequences of vectors and polynomials as before, if such sequences exist and ∞, otherwise. Theorem 1 implies

Corollary. *$M(n,d,K) < \infty$ if and only if either $n = 1$ or $\operatorname{char} K = 0$ or $\operatorname{char} K > d$. If K is infinite the same equivalence holds for $m(n,d,K)$.*

The problem of determination of $m(n,d,K)$ is related to the problem, much studied in the XIX th century (see [5], for a modern account), of representation of a general n-ary form of degree d as the sum of powers of linear forms. The two problems are not equivalent even for K algebraically closed, since in our case neither F nor f_μ are supposed homogeneous.

Theorem 2. *For every infinite field K such that $\operatorname{char} K = 0$ or $\operatorname{char} K > d$ we have*

$$\binom{n+d-1}{n-1} \ge M(n,d,K) \ge m(n,d,K) \ge \max_{0 \le e < d} \frac{1}{n+d-1-e}\left[\binom{n+d}{n} - \binom{n+e}{n}\right].$$

For $K = \mathbb{F}_q$, $\operatorname{char} K > d$, we have

$$\binom{n+d-1}{n-1} \ge M(n,d,K) \ge \max_{0 \le e < d} \frac{\left[\binom{n+d}{n} - \binom{n+e}{n}\right]\log q}{\log\left[(q^{d-e}-1)\frac{q^n-1}{q-1}+1\right]}.$$

In particular, every n-ary form of degree d over a field K of characteristic 0 is representable as a linear combination of $\binom{n+d-1}{n-1}$ d-th powers of linear forms over K. This has been first proved, but not explicitly stated by Ellison [3].

Clearly $M(1,d,K) = M(n,1,K) = 1$ and one easily proves

Theorem 3. *If $\operatorname{char} K \ne 2$, then $M(n,2,K) = n$ and if, in addition, K is infinite, then $m(n,2,K) = n$.*

Diaconis and Shahshahani asserted without a formal proof that $M(2,d,\mathbb{R}) = d$ ([2], Application 2).

We shall show

Theorem 4. *For every field K such that either* $\operatorname{char} K = 0$, *or* $\operatorname{char} K > d$ *and* $\operatorname{card} K \geq 2d - 2$ *we have*

$$M(2, d, K) = d.$$

In particular, every binary form F of degree d over a field K of characteristic 0 is representable as a linear combination of d d-th powers of linear forms over K, which slightly improves Theorem A of [4]. For $K = \mathbb{C}$ this was proved by Reznick [8].

The following theorem shows that the condition $\operatorname{card} K \geq 2d - 2$ in Theorem 4 may be superfluous.

Theorem 5. *For every field K such that*

$$\operatorname{char} K > d \textit{ and } \operatorname{card} K \leq d + 2$$

we have

$$M(2, d, K) = d.$$

Theorem 6. *For every algebraically closed field K, if* $\operatorname{char} K = 0$ *or* $\operatorname{char} K > d$, *then*

$$m(2, d, K) = \left\lceil \frac{2d + 5 - \sqrt{8d + 17}}{2} \right\rceil .$$

The proof of Theorem 1 is based on two lemmas.

Lemma 1. *Let $n \geq 2$, T_i $(1 \leq i \leq n-1)$ be a subset of K of cardinality $d+1$. Then $F = 0$ is the only polynomial in $K[x_1, \dots, x_{n-1}]$ of degree at most d in each variable such that $F(a_1, a_2, \dots, a_{n-1}) = 0$ for all $[a_1, a_2, \dots, a_{n-1}] \in T_1 \times \dots \times T_{n-1}$.*

Proof. See [1], Lemma 2.2.

Lemma 2. *Let for each $k = 0, 1, \dots, n-2$ elements $\beta_{k,l}$ of K $(0 \leq l \leq d)$ be distinct and let for a positive integer $q \leq (d+1)^{n-1}$*

$$q - 1 = \sum_{k=0}^{n-2} c_k(q)(d+1)^k, \quad \textit{where } c_k(q) \in \mathbb{Z}, \ 0 \leq c_k(q) \leq d$$

be the expansion of $q - 1$ in base $d + 1$.

Define

$$A((\beta_{kl})) \textit{ as the matrix } (a_{rs}), \textit{ where}$$

$$(2) \qquad a_{rs} = \prod_{k=0}^{n-2} \beta_{k,c_k(s)}^{c_k(r)} \ \left(1 \le r, s \le (d+1)^{n-1}\right).$$

Then det $A((\beta_{kl})) \neq 0$.

Proof. Let us put in Lemma 1: $T_i = \{\beta_{i-1,l} : 0 \le l \le d\}$ $(1 \le i \le n-1)$. By the lemma the only polynomial $F \in K[x_1, \dots, x_{n-1}]$ of degree at most d in each variable such that

$$(3) \quad F\left(\beta_{0,l_0}, \dots, \beta_{n-2,l_{n-2}}\right) = 0 \text{ for all } [l_0, \dots, l_{n-2}] \in \{0, 1, \dots, d\}^{n-1}$$

is $F = 0$.

Now, all the vectors $[l_0, \dots, l_{n-2}] \in \{0, 1, \dots, d\}^{n-1}$ can be ordered lexicographically, so that the vector $[l_0, \dots, l_{n-2}]$ occupies the position $1 + \sum_{i=0}^{n-2} l_i(d+1)^i$ and then the system of equations (3) reads

$$F\left(\beta_{0,c_0(r)}, \beta_{1,c_1(r)}, \dots, \beta_{n-2,c_{n-2}(r)}\right) = 0 \ \left(1 \le r \le (d+1)^{n-1}\right).$$

Also the polynomial F can be written as

$$\sum_{s=1}^{(d+1)^{n-1}} A_s \prod_{j=1}^{n-1} x_j^{c_{j-1}(s)}, \text{ where } A_s \in K$$

and (3) can be rewritten as

$$\sum_{s=1}^{(d+1)^{n-1}} A_s \prod_{j=0}^{n-2} \beta_{j,c_j(r)}^{c_j(s)} = 0 \ \left(1 \le r \le (d+1)^{n-1}\right).$$

The fact that the only solution of this system is

$$A_s = 0 \quad \left(1 \le r \le (d+1)^{n-1}\right),$$

corresponding to $F = 0$, implies in view of (2) that

$$\det\,(a_{sr}) \neq 0.$$

But then also det $A((\beta_{kl})) = \det\,(a_{rs}) \neq 0$.

Proof of Theorem 1. Let us choose in S_ν distinct elements $\beta_{\nu-2,0}, \dots, \beta_{\nu-2,d}$ $(2 \le \nu \le n)$. By Lemma 2

$$(4) \qquad \det A((\beta_{kl})) \neq 0,$$

hence the matrix B consisting of the rows r of $A((\beta_{kl}))$ for which $\sum_{k=0}^{n-2} c_k(r) \le d$ is of rank equal to the number of such rows $M = \binom{n+d-1}{n-1}$. Therefore B has M linearly independent columns $s_1, s_2, \dots, s_M$. We put

$$(5) \qquad \alpha_{\mu 1} = 1, \ \alpha_{\mu\nu} = \beta_{\nu-2,c_{\nu-2}(s_\mu)} \ (1 \le \mu \le M, \ 2 \le \nu \le n).$$

Let

$$(6) \qquad F(x_1,\dots,x_n) = \sum_{i_1+i_2+\cdots i_n \le d} \binom{i_1+\cdots+i_n}{i_1,\dots,i_n} a_{i_1\dots i_n} \prod_{j=1}^{n} x_j^{i_j}$$

(note that the multinomial coefficient is non-zero).

For each $l \le d$ we determine $b_{\mu l}$ $(1 \le \mu \le M)$ from the system of equations

$$(7) \qquad \sum_{\mu=1}^{M} b_{\mu l} \prod_{\nu=2}^{n} \alpha_{\mu\nu}^{i_\nu} = a_{i_1\dots i_n} \ (i_1+\cdots+i_n = l),$$

which can be rewritten as

$$\sum_{\mu=1}^{M} b_{\mu l} \prod_{\nu=0}^{n-2} \beta_{\nu,c_\nu(s_\mu)}^{c_\nu(r)} = a_{l-\sum_{\nu=0}^{n-2} c_\nu(r),c_0(r),\dots,c_{n-2}(r)}$$
$$\left(1 \le r \le (d+1)^{n-1},\ \sum_{\nu=0}^{n-2} c_\nu(r) \le l\right).$$

By the choice of $s_1,\dots,s_M$ the matrix of this system has rank equal to the number of equations, hence the system is solvable for $b_{\mu l} \in K$. We set

$$f_\mu = \sum_{l=0}^{d} b_{\mu l} z^l$$

and (1) follows from (6) and (7).

Proof of Corollary. In view of Theorem 1 it is sufficient to show that $M(n,d,K) = \infty$ if $n > 1$ and

$$0 < p = \operatorname{char} K \le d.$$

Let us consider an arbitrary polynomial F of the form (6) in which $a_{d,0,\dots,0} \ne 0$ and $a_{p-1,1,0,\dots,0} \ne 0$. If K is infinite such polynomials exist in every open subset of $P(n,d,K)$. If (1) holds, then the part F_{d-p} of degree p of F satisfies

$$F_{d-p} = \sum_{\mu=1}^{M} b_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu\right)^p, \ b_\mu \in K,$$

which is impossible, since $x_1^{p-1}x_2$ occurs with a non-zero coefficient on the left-hand side, but not on the right.

Proof of Theorem 2. The dimension of the set of all n-ary polynomials of degree not exceeding d and greater than e is $\binom{n+d}{d} - \binom{n+e}{e}$. On the other hand, the dimension of the set of all polynomials of the form $f(\alpha x)$, where $f = \sum_{l=e+1}^{d} b_l z^l$ is at most $d - e + n - 1$ since the vectors $\boldsymbol{\alpha}$ can be normalized by taking the first non-vanishing coordinate equal to 1. This gives the upper bound $m(n + d - 1 - e)$ for the dimension of the set of all polynomials of the form $\sum_{\mu=1}^{m} f_\mu(\boldsymbol{\alpha}_\mu \boldsymbol{x})$ and, by the definition of $m(n, d, K)$

$$m(n, d, K)(n + d - 1 - e) \geq \binom{n+d}{d} - \binom{n+e}{e},$$

which implies the first part of the theorem.

In order to prove the second part let us observe that the number of normalized vectors $\boldsymbol{\alpha} \in \mathbb{F}_q^n$ is $\frac{q^n-1}{q-1}$, while the number of non-zero polynomials $\sum_{l=e+1}^{d} b_l z^l \in \mathbb{F}_q[z]$ is $q^{d-e} - 1$. Hence we obtain at most $(q^{d-e} - 1)\frac{q^n-1}{q-1} + 1$ polynomials of the form $f(\boldsymbol{\alpha x})$ and at most $\left((q^{d-e} - 1)\frac{q^n}{q-1} + 1\right)^m$ polynomials of the form $\sum_{\mu=1}^{m} f_\mu(\boldsymbol{\alpha}_\mu \boldsymbol{x})$. On the other hand, the number of n-ary polynomials over $\mathbb{F}_q$ of degree not exceeding d and greater than e is

$$q^{\binom{n+d}{d}-\binom{n+e}{e}}.$$

By the definition of $M(n, d, \mathbb{F}_q)$ this gives

$$M(n, d, \mathbb{F}_q) \log\left(\left(q^{d-e} - 1\right)\frac{q^n - 1}{q - 1} + 1\right) \geq \left(\binom{n+d}{d} - \binom{n+e}{e}\right) \log q,$$

which implies the second part of the theorem.

Proof of Theorem 3. Let F_0, the leading quadratic form of F, be of rank r. By Lagrange's theorem there exist linearly independent vectors $[\alpha_{\mu 1}, \dots, \alpha_{\mu n}]$ in K^n $(1 \leq \mu \leq r)$ such that

$$F_0 = \sum_{\mu=1}^{r} a_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu\right)^2, \quad a_\mu \in K.$$

We set $a_\mu = 0$ for $r < \mu \leq n$ and choose $n - r$ vectors $[\alpha_{\mu 1}, \dots, \alpha_{\mu n}]$ in K^n $(1 \leq \mu \leq r)$ such that $\det(\alpha_{\mu\nu})_{\mu,\nu \leq n} \neq 0$. Then there exist $b_\mu \in K$ $(1 \leq \mu \leq n)$ such that

$$F - F_0 - F(0, \dots, 0) = \sum_{\mu=1}^{n} b_\mu \sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu$$

and (1) follows with $M = n$

$$f_1(z) = a_1z^2 + b_1z + F(0,\dots,0),$$
$$f_\mu(z) = a_\mu z^2 + b_\mu z \quad (1 < \mu \le n).$$

On the other hand, the polynomial $F = \sum_{\nu=1}^{n} c_\nu x_\nu^2$ where $c_\nu \ne 0$ is clearly not representable in the form (1) with $M < n$.

For the proof of Theorem 4 we need

Lemma 3. *We have the identity*

$$\begin{vmatrix} 1\dots & 1 & A_0 \\ x_1\dots & x_d & A_1 \\ \vdots & \vdots & \vdots \\ x_1^d\dots & x_d^d & A_d \end{vmatrix} = \prod_{1\le i<j\le d} (x_j - x_i) \sum_{i=0}^{d} (-1)^i A_{d-i} \tau_i (x_1,\dots,x_d),$$

where τ_i is the i-th fundamental symmetric function of $x_1,\dots,x_d$, $\tau_0 = 1$.

Proof . See [7], p. 333.

Lemma 4. *Let $\boldsymbol{\alpha}_\mu$ $(1 \le \mu \le d)$ be arbitrary pairwise linearly independent vectors in K^2. If* $\operatorname{char} K = 0$ *or* $\operatorname{char} K \ge d$*, for every polynomial $F \in K[x_1, x_2]$ of degree at most $d - 1$ there exist polynomials $f_\mu \in K[z]$ such that*

$$F = \sum_{\mu=1}^{d} f_\mu (\alpha_{\mu 1}x_1 + \alpha_{\mu 2}x_2).$$

Proof . Since $\boldsymbol{\alpha}_\mu$ are pairwise linearly independent we may assume that either

(i) $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ are all distinct $(1 \le \mu \le d)$,

or (ii) $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ are all distinct $(1 \le \mu < d)$, $\alpha_{d1} = 0, \alpha_{d2} = 1$.

Let now

$$F = \sum_{i_1+i_2<d} \binom{i_1+i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2}$$

(note that the binomial coefficient is non-zero). In the case (i) for each $l < d$ we can solve for $b_{\mu l}$ in K the system of equations

$$a_{l-i,i} = \sum_{\mu=1}^{d} b_{\mu l}\alpha_{\mu 2}^i \ (0 \le i \le l),$$

since the rank of the matrix of the coefficients equals the number of equations. Then we set

$$f_\mu(z)=\sum_{l=0}^{d-1} b_{\mu l}z^l.$$

In the case (ii) for each $l<d$ we can solve for $b_{\mu l}$ in K the system of equations

$$a_{l-i,i}=\sum_{\mu=1}^{d-1} b_{\mu l}\alpha_{\mu 2}^i \ (0\le i<l),$$

and then we set

$$f_\mu(z)=\sum_{l=0}^{d-1} b_{\mu l}z^l \ (\mu<d), f_d(z)=\sum_{l=0}^{d-1}\left(a_{0l}-\sum_{\mu=1}^{d-1} b_{\mu l}\alpha_{\mu 2}^l\right)z^l.$$

Proof of Theorem 4. In view of Theorem 3 we may assume $d\ge 3$. We shall prove first that

$$M(2,d,K)\le d.$$

Let $F\in P(2,d,K)$ and let F_0 be the highest homogeneous part of F. Supposing that we have represented F_0 in the form (1) with $M=d$ we may assume that $\boldsymbol{\alpha}_\mu$ $(1\le\mu\le d)$ are pairwise linearly independent and then apply Lemma 4 to represent $F-F_0$ in the form (1) with the same $\boldsymbol{\alpha}_\mu$. Therefore, it is enough to find a representation (1) for F homogeneous of degree d. By Lemma 1 there exist c_{11},c_{21} in K such that $F(c_{11},c_{21})\ne 0$. Replacing F by $F(c_{11}x_1+c_{12}x_2, c_{21}x_1+c_{22}x_2)$, where c_{12},c_{22} are chosen in K so that $c_{11}c_{22}-c_{12}c_{21}\ne 0$ we may assume that the coefficient of x_1^d in $F(x_1,x_2)$ is non-zero. Let then

$$F(x_1,x_2)=\sum_{i=0}^{d}\binom{d}{i}a_i x_1^{d-i}x_2^i,\ a_0\ne 0 \tag{8}$$

and let us consider the polynomial

$$\begin{aligned}G(y_1,\dots,y_{d-2})={}&\prod_{1\le i<j\le d-2}(y_j-y_i)\cdot\sum_{i=2}^{d}(-1)^{i-1}a_{d-i}\tau_{i-2}(y_1,\dots,y_{d-2})\\&\cdot\prod_{j=1}^{d-2}\Bigg(a_{d-1}+\sum_{i=2}^{d-1}(-1)^{i-1}a_{d-i}\big(\tau_{i-1}(y_1,\dots,y_{d-2})+y_j\tau_{i-2}(y_1,\dots,y_{d-2})\big)\\&\quad+(-1)^{d-1}a_0y_j\tau_{d-2}(y_1,\dots,y_{d-2})\Bigg).\end{aligned}$$

Since $a_0\ne 0$ the polynomial G is not identically 0 and we have for each $i\le d-2$

$$\deg_{y_i}G=2d-3.$$

Since card $K \geq 2d-2$, by Lemma 1 there exist elements $\beta_1, \dots, \beta_{d-2}$ of K such that

$$G(\beta_1, \dots, \beta_{d-2}) \neq 0. \tag{9}$$

We now put

$$\beta_{d-1} = -\frac{\sum_{i=1}^{d-1} (-1)^{i-1} a_{d-i} \tau_{i-1}(\beta_1, \dots, \beta_{d-2})}{\sum_{i=2}^{d} (-1)^{i-1} a_{d-i} \tau_{i-2}(\beta_1, \dots, \beta_{d-2})}, \tag{10}$$

which makes sense, since by (9) the denominator is non-zero. Again by (9) we have $\beta_i \neq \beta_j$ for $1 \leq i < j < d$. Hence

$$D_0 = \begin{vmatrix} 1 \dots & 1 \\ \beta_1 \dots & \beta_{d-1} \\ \vdots & \vdots \\ \beta_1^{d-2} \dots & \beta_{d-1}^{d-2} \end{vmatrix} = \prod_{1 \leq i < j < d} (\beta_j - \beta_i) \neq 0.$$

However, by (10) and Lemma 3,

$$\begin{aligned} D = \begin{vmatrix} 1 \dots & 1 & a_0 \\ \beta_1 \dots & \beta_{d-1} & a_1 \\ \vdots & \vdots & \vdots \\ \beta_1^{d-1} \dots & \beta_{d-1}^{d-1} & a_{d-1} \end{vmatrix} \\ = \prod_{1 \leq i < j < d} (\beta_j - \beta_i) \cdot \sum_{i=1}^{d} (-1)^{i-1} a_{d-i} \tau_{i-1}(\beta_1, \dots, \beta_{d-1}) \\ = D_0 \Bigg(a_{d-1} + \sum_{i=2}^{d-1} (-1)^{i-1} a_{d-i} \big(\beta_{d-1} \tau_{i-2}(\beta_1, \dots, \beta_{d-2}) \\ + \tau_{i-1}(\beta_1, \dots, \beta_{d-2}) \big) + (-1)^{d-1} a_0 \beta_{d-1} \tau_{d-2}(\beta_1, \dots, \beta_{d-2}) \Bigg) = 0. \end{aligned}$$

Hence the system of equations

$$\sum_{\mu=1}^{d-1} b_\mu \beta_\mu^j = a_j \ (0 \leq j < d) \tag{11}$$

is solvable for elements b_μ of K.

We set

$$\alpha_{\mu 1} = 1,\ \alpha_{\mu 2} = \beta_\mu,\ f_\mu(z) = b_\mu z^d,\ (1 \le \mu < d);$$
$$\alpha_{d1} = 0,\ \alpha_{d2} = 1,\ f_d(z) = \left(a_d - \sum_{\mu=1}^{d-1} b_\mu \beta_\mu^d\right) z^d$$

and obtain (1) from (8) and (11).

It remains to show that $M(2,d,K) \ge d$. Let us consider the equation

$$x_1 x_2^{d-1} + a x_2^d = \sum_{\mu=1}^{d-1} f_\mu\left(\alpha_{\mu 1} x_1 + \alpha_{\mu 2} x_2\right). \tag{12}$$

In order to prove that it is impossible for every $a \in K$ it is clearly sufficient to consider $f_\mu = b_\mu z^d$, $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ distinct. Comparing the coefficients of $x_1^{d-j} x_2^j$ on both sides of (12) we obtain

$$0 = \sum_{\mu=1}^{d-1} b_\mu \alpha_{\mu 2}^j \quad (0 \le j < d-1).$$

The determinant of this system is $\prod_{1 \le \mu < \nu < d} (\alpha_{\nu 2} - \alpha_{\mu 2}) \ne 0$, hence $b_\mu = 0$ $(1 \le \mu < d)$ and by (12)

$$x_1 x_2^{d-1} + a x_2^d = 0,$$

a contradiction. This argument is valid without the assumption on card K.

For the proof of Theorem 5 we need

Lemma 5. *Let $a_1, \dots, a_k$ be distinct elements of $\mathbb{F}_p^*$, $k \ge p-3$. Then*

$$\tau_j(a_1, \dots, a_k) = \begin{cases} 0 & \text{if } k = p-1,\ 0 < j < k \\ (-r)^j & \text{if } \begin{array}{l} 0 \le j \le k = p-2, \text{ and} \\ \{r\} = \mathbb{F}_p^* \setminus \{a_1, \dots, a_k\} \end{array} \\ (-1)^j \frac{r^{j+1} - s^{j+1}}{r-s} & \text{if } \begin{array}{l} 0 \le j \le k = p-3, \text{ and} \\ \{r, s\} = \mathbb{F}_p^* \setminus \{a_1, \dots, a_k\} \end{array} \end{cases}$$

Proof. If $k = p-1$ we use the identity

$$x^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^*} (x - a).$$

If $k = p-2$ we argue by induction. For $j = 0$ the statement is true, for $k \ge j \ge 1$ we have the identity

$$0 = \tau_j(a_1, \dots, a_k, r) = \tau_j(a_1, \dots, a_k) + r\tau_{j-1}(a_1, \dots, a_k),$$

hence, by induction

$$\tau_j(a_1,\dots,a_k) = -r\tau_{j-1}(a_1,\dots,a_k) = -r(-r)^{j-1} = (-r)^j.$$

If $k = p-3$ we argue again by induction. If $j = 0$ the statement is true. If $k \ge j \ge 1$ we have the identity

$$(-r)^j = \tau_j(a_1,\dots,a_k,s) = \tau_j(a_1,\dots,a_k) + s\tau_{j-1}(a_1,\dots,a_k),$$

hence, by induction

$$\tau_j(a_1,\dots,a_k) = (-r)^j - s\tau_{j-1}(a_1,\dots,a_k) = (-1)^j r^j + (-1)^j s\frac{r^j - s^j}{r-1}$$
$$= (-1)^j \frac{r^{j+1} - s^{j+1}}{r-s}.$$

Proof of Theorem 5. By the last statement in the proof of Theorem 4 we have $M(2,d,K) \ge d$, thus it is remains to prove the reverse inequality. Let $F \in P(2,d,K)$. By Lemma 4 we may assume that F is homogeneous. Let

$$F(x_1,x_2) = \sum_{i=0}^{d} \binom{d}{i} a_i x_1^{d-i} x_2^i \tag{13}$$

and consider first $\operatorname{card} K = p = d+1$.

Let us assume first that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t) = \sum_{i=0}^{p-1} a_{p-1-i}t^i$ is not injective. Then there exist $r, s \in \mathbb{F}_p^*$ such that $r \ne s$ and $f(r) = f(s)$, hence

$$\sum_{i=1}^{p-2} a_{p-1-i}\frac{r^i - s^i}{r-s} = 0. \tag{14}$$

Setting $\alpha_{12} = 0$, $\{\alpha_{22},\dots,\alpha_{p-2,2}\} = \mathbb{F}_p^* \setminus \{r,s\}$ we have by Lemma 5

$$\tau_i(\alpha_{12},\dots,\alpha_{p-2,2}) = \tau_i(\alpha_{22},\dots,\alpha_{p-2,2}) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r-s} \quad (i \le p-3),$$
$$\tau_{p-2}(\alpha_{12},\dots,\alpha_{p-2,2}) = 0,$$

hence, by (14),

$$\sum_{i=1}^{p-1} (-1)^{i-1} a_{p-1-i}\tau_{i-1}(\alpha_{12},\dots,\alpha_{p-2,2}) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1\dots & 1 & a_0 \\ \alpha_{12}\dots & \alpha_{p-2,2} & a_1 \\ \vdots & \vdots & \vdots \\ \alpha_{12}^{p-2}\dots & \alpha_{p-2,2}^{p-2} & a_{p-2} \end{vmatrix} = 0.$$

Since $\det\left(\alpha_{\mu 2}^{j}\right)_{\substack{0\le j<p-2\\ 1\le\mu\le p-2}}\neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-2} b_\mu \alpha_{\mu 2}^{j} = a_j \ (0\le j<p-1). \tag{15}$$

Then we obtain from (13) - (15) that

$$F(x_1,x_2)=\sum_{\mu=1}^{p-2} b_\mu \left(x_1+\alpha_{\mu 2}x_2\right)^{p-1}+\left(a_{p-1}-\sum_{\mu=1}^{p-2} b_\mu\alpha_{\mu 2}^{p-1}\right)x_2^{p-1}.$$

Assume now that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t\mapsto f(t)$ is injective. We shall consider three cases

(i) $\quad a_0\in f\left(\mathbb{F}_p^*\right)$,

(ii) $\quad a_{p-1}\in f\left(\mathbb{F}_p^*\right)$,

(iii) $\quad a_{p-1}\notin f\left(\mathbb{F}_p^*\right),\ a_0\notin f\left(\mathbb{F}_p^*\right)$.

In the case (i), let

$$a_0=f(r),\ r\in\mathbb{F}_p^*,$$

so that

$$\sum_{i=0}^{p-2} a_{p-1-i} r^{i}=0. \tag{16}$$

Setting $\alpha_{12}=0$, $\{\alpha_{22},\dots,\alpha_{p-1,2}\}=\mathbb{F}_p^*\setminus\{r\}$ we have by Lemma 5

$$\begin{aligned}&\tau_i\left(\alpha_{12},\dots,\alpha_{p-1,2}\right)=\tau_i\left(\alpha_{22},\dots,\alpha_{p-1,2}\right)=(-r)^i(i\le p-2),\\&\tau_{p-1}\left(\alpha_{12},\dots,\alpha_{p-1,2}\right)=0,\end{aligned}$$

hence, by (16),

$$\sum_{i=0}^{p-1}(-1)^i a_{p-1-i}\tau_i\left(\alpha_{12},\dots,\alpha_{p-1,2}\right)=0$$

and, by Lemma 3,

$$\begin{vmatrix} 1\dots & 1 & a_0\\ \alpha_{12}\dots & \alpha_{p-1,2} & a_1\\ \vdots & \vdots & \vdots\\ \alpha_{12}^{p-1}\dots & \alpha_{p-1,2}^{p-1} & a_{p-1}\end{vmatrix}=0.$$

Since $\det\left(\alpha_{\mu 2}^{j}\right)_{\substack{0\le j<p-1\\ 1\le\mu\le p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \alpha_{\mu 2}^{j} = a_j \ (0 \le j \le p-1). \tag{17}$$

Then we obtain from (13) and (17) that

$$F(x_1, x_2) = \sum_{\mu=1}^{p-1} b_\mu \left(x_1 + \alpha_{\mu 2} x_2\right)^{p-1}.$$

In the case (ii), let

$$a_{p-1} = f\left(r^{-1}\right),\ r \in \mathbb{F}_p^*,$$

so that

$$\sum_{i=0}^{p-2} a_i r^i = \sum_{i=1}^{p-1} a_{p-1-i} r^{p-1-i} = 0. \tag{18}$$

Setting $\alpha_{11} = 0$, $\{\alpha_{21}, \ldots, \alpha_{p-1,1}\} = \mathbb{F}_p^* \setminus \{r\}$ we have by Lemma 5

$$\begin{aligned}
&\tau_i(\alpha_{11}, \ldots, \alpha_{p-1,1}) = \tau_i(\alpha_{21}, \ldots, \alpha_{p-1,1}) = (-r)^i \ (i \le p-2),\\
&\tau_{p-1}(\alpha_{11}, \ldots, \alpha_{p-1,1}) = 0,
\end{aligned}$$

hence, by (18),

$$\sum_{i=0}^{p-1} (-1)^i a_i \tau_i(\alpha_{11}, \ldots, \alpha_{p-1,1}) = 0$$

and, by Lemma 3,

$$\begin{vmatrix}
1 \ldots & 1 & a_{p-1}\\
\alpha_{11} \cdots & \alpha_{p-1,1} & a_{p-2}\\
\vdots & \vdots & \vdots\\
\alpha_{11}^{p-1} \cdots & \alpha_{p-1,1}^{p-1} & a_0
\end{vmatrix} = 0.$$

Since $\det\left(\alpha_{\mu 1}^{j}\right)_{\substack{0\le j<p-1\\ 1\le\mu\le p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \alpha_{\mu 1}^{j} = a_{p-1-j} \ (0 \le j \le p-1). \tag{19}$$

Then we obtain from (13) and (19)

$$F(x_1, x_2) = \sum_{l=0}^{p-1} b_\mu \left(\alpha_{\mu 1} x_1 + x_2\right)^{p-1}.$$

In the case (iii), since

$$\operatorname{card} f\left(\mathbb{F}_p^*\right) = \operatorname{card} \mathbb{F}_p^* = p-2$$

we have $a_0 = a_{p-1}$. Hence the first and the last row of the determinant

$$\begin{vmatrix} 1\dots & 1 & a_0 \\ 1\dots & p-1 & a_1 \\ \vdots & \vdots & \vdots \\ 1^{p-1}\dots & (p-1)^{p-1} & a_{p-1} \end{vmatrix}.$$

are equal and the determinant vanishes.

Since $\det\left(\mu^j\right)_{\substack{0\le j<p-1 \\ 1\le\mu\le p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \mu^j = a_j \ (0 \le j \le p-1). \tag{20}$$

Then we obtain from (13) and (20)

$$F(x_1, x_2) = \sum_{\mu=1}^{p-1} b_\mu \left(x_1 + \mu x_2\right)^{p-1}.$$

Consider now the case, where

$$\operatorname{card} K = p = d+2.$$

Again, let us assume first that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t) = \sum_{i=0}^{p-2} a_{p-2-i} t^i$ is not injective. Then there exist $r, s \in \mathbb{F}_p^*$ such that $r \neq s$ and $f(r) = f(s)$, hence

$$\sum_{i=1}^{p-2} a_{p-2-i} \frac{r^i - s^i}{r-s} = 0. \tag{21}$$

Setting $\{\alpha_{12}, \dots, \alpha_{p-3,2}\} = \mathbb{F}_p^* \setminus \{r, s\}$ we have by Lemma 5

$$\tau_i\left(\alpha_{12}, \dots, \alpha_{p-3,2}\right) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r-s} \quad (i \le p-3)$$

hence, by (21),

$$\sum_{i=1}^{p-2} (-1)^{i-1} a_{p-2-i} \tau_{i-1}\left(\alpha_{12}, \dots, \alpha_{p-3,2}\right) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1\dots & 1 & a_0 \\ \alpha_{12}\cdots & \alpha_{p-3,2} & a_1 \\ \vdots & \vdots & \vdots \\ \alpha_{12}^{p-3}\cdots & \alpha_{p-3,2}^{p-3} & a_{p-3} \end{vmatrix} = 0.$$

Since $\det\left(\alpha_{\mu 2}^{j}\right)_{\substack{0\le j<p-3\\ 1\le\mu\le p-3}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$(22)\qquad \sum_{\mu=1}^{p-3} b_\mu \alpha_{\mu 2}^{j} = a_j \ (0\le j<p-2).$$

Then we obtain from (13) and (22) that

$$F(x_1,x_2) = \sum_{\mu=1}^{p-3} b_\mu \left(x_1+\alpha_{\mu 2}x_2\right)^{p-2} + \left(a_{p-2}-\sum_{\mu=1}^{p-3} b_\mu \alpha_{\mu 2}^{p-2}\right) x_2^{p-2}.$$

Assume now that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t)$ is injective. We shall consider two cases

$$\text{(iv)}\qquad 0\in f\left(\mathbb{F}_p^*\right),$$

$$\text{(v)}\qquad 0\notin f\left(\mathbb{F}_p^*\right).$$

In the case (iv) let $0=f(r)$, $r\in\mathbb{F}_p^*$, so that

$$(23)\qquad \sum_{i=0}^{p-2} a_{p-2-i} r^i = 0.$$

Setting $\{\alpha_{12},\dots,\alpha_{p-2,2}\} = \mathbb{F}_p^*\setminus\{r\}$ we have by Lemma 5

$$\tau_i\left(\alpha_{12},\dots,\alpha_{p-2,2}\right) = (-r)^i \ (1\le i\le p-2),$$

hence, by (23)

$$(24)\qquad \sum_{i=0}^{p-2}(-1)^i a_{p-2-i}\tau_i\left(\alpha_{12},\dots,\alpha_{p-2,2}\right) = 0$$

and by Lemma 3

$$\begin{vmatrix} 1\dots & 1 & a_0 \\ \alpha_{12}\cdots & \alpha_{p-2,2} & a_1 \\ \vdots & \vdots & \vdots \\ \alpha_{12}^{p-2}\cdots & \alpha_{p-2,2}^{p-2} & a_{p-2} \end{vmatrix} = 0.$$

Since $\det\left(\alpha_{\mu 2}^{j}\right)_{\substack{0\le j<p-2\\ 1\le\mu\le p-2}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-2} b_\mu \alpha_{\mu 2}^{j} = a_j \ (0 \le j \le p-2). \tag{25}$$

Then we obtain from (13) and (25) that

$$F(x_1, x_2) = \sum_{\mu=1}^{p-2} b_\mu \left(x_1 + \alpha_{\mu 2} x_2\right)^{p-2}.$$

In the case (v) $t \mapsto f(t)$ is a bijective mapping of $\mathbb{F}_p^*$ onto $\mathbb{F}_p^*$. If the mapping $t \mapsto tf(t)$ had the same property, we should obtain

$$-1 = \prod_{t\in\mathbb{F}_p^*} tf(t) = \prod_{t\in\mathbb{F}_p^*} t \cdot \prod_{t\in\mathbb{F}_p^*} f(t) = (-1)^2 = 1,$$

which is impossible. Hence there exist $r, s \in \mathbb{F}_p^*$ such that $r \neq s$ and $rf(r) = sf(s)$:

$$\sum_{i=0}^{p-2} a_{p-2-i} \frac{r^{i+1} - s^{i+1}}{r-s} = 0. \tag{26}$$

Setting

$$\alpha_{12} = 0, \ \{\alpha_{22}, \dots, \alpha_{p-2,2}\} = \mathbb{F}_p^* \setminus \{r, s\}$$

we have by Lemma 5

$$\begin{aligned} &\tau_i\left(\alpha_{12}, \dots, \alpha_{p-2,2}\right) = \tau_i\left(\alpha_{22}, \dots, \alpha_{p-2,2}\right) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r-s}, \\ &\tau_{p-2}\left(\alpha_{12}, \dots, \alpha_{p-2,2}\right) = 0, \end{aligned}$$

hence, by (26), (24) holds and we conclude the argument as in the case (iv). The proof of Theorem 5 is complete.

Proof of Theorem 6. We shall prove first that

$$m(2, d, K) \ge \left\lceil \frac{2d + 5 - \sqrt{8d+17}}{2} \right\rceil =: m. \tag{27}$$

Let $2d + 4 = u^2 + v$, where u, v are integers, $|v| \le u$. We have

$$\left(u + \frac{2d+4}{u}\right)^2 = \left(2u + \frac{v}{u}\right)^2 \le 4u^2 + 4v + 1 = 8d + 17,$$

hence on taking $e = d + 1 - u$ we obtain from Theorem 2

$$m(2,d,K) \geq \frac{1}{d+1-e}\left[\binom{d+2}{2} - \binom{e+2}{2}\right] = \\ = \frac{(u-1)(2d+5-u)}{2u} \geq \frac{2d+5-\sqrt{8d+17}}{2},$$

which gives (27).

In order to show that

$$m(2,d,K) \leq m$$

we notice that

$$\rho := m - \binom{d-m+2}{2} \geq 0.$$

Let us consider independent variables $a_{i,j}$, where $i, j \geq 0$, $m \leq i + j \leq d$ and the matrix $B = (b_{\mu\nu})_{\substack{1 \leq \mu \leq m-\rho \\ 0 \leq \nu \leq m-\rho}}$, where

$$b_{\mu 0} = a_{\binom{k_\mu+1}{2}-\mu,\ m-\binom{k_\mu}{2}-1+\mu}$$
$$b_{\mu\nu} = a_{\rho+\binom{k_\mu+1}{2}+\nu-\mu,\ m-\rho-\binom{k_\mu}{2}-1+\mu-\nu} \ (1 \leq \nu \leq m-\rho),$$

k_μ being determined by the inequality

$$\binom{k_\mu}{2} < \mu \leq \binom{k_\mu+1}{2}.$$

Let B_ν be the minor of the matrix B obtained by omitting the ν-th column and D be the discriminant of the polynomial

$$B_0 x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu B_\nu x^{m-\rho-\nu}.$$

Polynomials B_0 and D in the variables a_{ij} are not identically zero.

In order to see that $B_0 \neq 0$ let us order all variables a_{ij} linearly assuming $a_{ij} \prec a_{kl}$ if either $i + j < k + l$ or $i + j = k + l$ and $j < l$. Then all products of a_{ij} are ordered lexicographically. The product

$$\pm \prod_{\mu+\nu=m-\rho+1} b_{\mu\nu} = \pm \prod_{\mu=1}^{m-\rho} a_{m+\binom{k_\mu+1}{2}+1-2\mu,2\mu-\binom{k_\mu}{2}-2}$$

occuring in the expansion of B_0 precedes in the lexicographic order any other term in this expansion, hence it does not cancel and $B_0 \neq 0$. On the other hand

$$D = B_0^{2m-2} D_0,$$

where D_0 is the discriminant of the polynomial

$$x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu \frac{B_\nu}{B_0} x^{m-\rho-\nu}.$$

Now, the discriminant of the polynomial

$$x^m - \sum_{\nu=1}^{m-\rho} t_\nu x^{m-\rho-\nu}$$

is not identically 0 as a function of t_ν (it is different from 0 for $t_\nu = 0$ for $\nu < m-\rho$, $t_{m-\rho} = 1$), hence $D_0 = 0$ implies an algebraic dependence over the prime field Π of K between $(-1)^{\nu-1}B_\nu/B_0$ $(1 \le \nu \le m-\rho)$. Let

$$\Omega = \Pi\left(a_{m+k-1-j,j} :\ 1 \le k \le d-m+1,\ 0 \le i \le m+k-1\right).$$

We assert that for $1 \le k \le d-m+1$, $0 \le i \le m+k-1$

$$a_{m+k-1-i,i} \in \Omega\left(\frac{B_1}{B_0}, \dots, \frac{B_{m-\rho}}{B_0}\right). \tag{28}$$

This is obviously true for $i \le m-1$. Assume that it is true for all $i < j$, where $m \le j \le m+k-1$. Since, by the Cramer formulae, for $\mu = \binom{k}{2} + j - m + 1 \le \binom{k+1}{2}$

$$\begin{aligned}\sum_{\nu=1}^{m-\rho}(-1)^{\nu-1}\frac{B_\nu}{B_0}a_{\rho+\binom{k+1}{2}+\nu-\mu,m-\rho-\binom{k}{2}-1+\mu-\nu} &= a_{\binom{k+1}{2}-\mu,\ m-\binom{k}{2}-1+\mu}\\ &= a_{k-j+m-1,j}\end{aligned} \tag{29}$$

and all a's occuring on the left-hand side have the second index at most

$$m-\rho-\binom{k}{2}-1+\binom{k}{2}+j-m+1-1 = j-\rho-1 < j,$$

it follows that $a_{m+k-1-j,j} \in \Omega\left(\frac{B_1}{B_0}, \dots, \frac{B_{m-\rho}}{B_0}\right)$ and the inductive proof of (28) is complete. But then

$$\operatorname{tr.deg}.\Omega\left(\frac{B_1}{B_0}, \dots, \frac{B_{m-\rho}}{B_0}\right)/\Omega < m-\rho$$

implies

$$\operatorname{tr.deg}.\Omega\left(a_{m+k-1-j,j} :\ 1 \le k \le d-m+1,\ m \le j \le m+k-1\right)/\Omega < m-\rho,$$

while the number of independent variables $a_{m+k-1-j,j}$ $(1 \le k \le d-m+1,\ m \le j \le m+k-1)$ equals

$$\sum_{k=1}^{d-m+1} k = \binom{d-m+2}{2} = m-\rho.$$

The obtained contradiction shows that $D_0 \ne 0$, and hence $D \ne 0$.

We now assert that if for a polynomial

$$F = \sum_{i_1+i_2 \le d} \binom{i_1+i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \tag{30}$$

we have $B_0 D \neq 0$, then there exist $f_\mu \in K[z]$ and $\alpha_\mu \in K (1 \le \mu \le m)$ such that

$$F(x_1, x_2) = \sum_{\mu=1}^{m} f_\mu (x_1 + \alpha_\mu x_2). \tag{31}$$

Indeed, using the notation introduced earlier we take for α_μ $(1 \le \mu \le m)$ the m distinct zeros of the polynomial

$$B_0 x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu B_\nu x^{m-\rho-\nu}.$$

Now for each $l \le d$ we solve the system of equations

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i = a_{l-i,i} \ (0 \le i \le \min(l, m-1))$$

for $b_{\mu l}$ in K and assert that the solution satisfies the larger system

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^j = a_{l-j,j} \ (0 \le j \le l). \tag{32}$$

The proof is by induction on j. We assume that (32) is true for all $j < i$, where $l \ge i \ge m$ and obtain

$$\begin{aligned} \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i &= \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^{i-m} \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} \alpha_\mu^{m-\rho-\nu} \\ &= \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^{i-\rho-\nu} = \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} a_{l-i+\rho+\nu, i-\rho-\nu}. \end{aligned} \tag{33}$$

However the sum on the right-hand side of (33) coincides with the sum on the left-hand side of (29) on putting there $k = l-m+1$, $\mu = i-m+\binom{k}{2}+1 \le \binom{k+1}{2}$. Hence by (29)

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i = a_{\binom{k+1}{2}-\mu,\ m-\binom{k}{2}-1+\mu} = a_{l-i,i}$$

which proves (32).

Now, on taking

$$f_\mu(z) = \sum_{l=0}^{d} b_{\mu l} z^l,$$

we obtain (31) from (30) and (32).

Example. Each three of the vectors $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[3,1,1]$, $[1,3,1]$, $[3,3,2]$ are linearly independent over $\mathbb{Q}$, nevertheless for all polynomials $f_i \in \mathbb{Q}[z]$ $(1 \le i \le 6)$ we have

$$3x_1x_2 + 2x_1x_3 \ne \sum_{i=1}^{3} f_i(x_i) + f_4(3x_1 + x_2 + x_3) + f_5(x_1 + 3x_2 + x_3) + f_6(3x_1 + 3x_2 + 2x_3).$$

Indeed, it is enough to consider the case $f_i = b_i z^2$ $(1 \le i \le 6)$. Assuming the equality in (33) we obtain comparing the coefficients of x_1x_2, x_1x_3 and x_2x_3

$$\begin{aligned} 6b_4 + 6b_5 + 18b_6 &= 3, \\ 6b_4 + 2b_5 + 12b_6 &= 2, \\ 2b_4 + 6b_5 + 12b_6 &= 0, \end{aligned}$$

which is impossible, since

$$\begin{vmatrix} 6 & 6 & 18 \\ 6 & 2 & 12 \\ 2 & 6 & 12 \end{vmatrix} = 0, \qquad \begin{vmatrix} 6 & 6 & 3 \\ 6 & 2 & 2 \\ 2 & 6 & 0 \end{vmatrix} \ne 0.$$

I conclude by expressing my thanks to U. Zannier for a remark helpful in the proof of Theorem 5.

Note added in proof. M. Kula has checked that M(2,d,K) = d in the simplest cases not covered by Theorems 4 and 5: $d = 7$ or 8, $K = \mathbb{F}_{11}$.

References

[1] N. ALON, M. B. NATHANSON, I. RUZSA, *The polynomial method and restricted sums of congruence classes.* J. Number Theory **56** (1996), 404–417.

[2] P. DIACONIS, M. SHAHSHAHANI, *On nonlinear functions of linear combinations.* SIAM J. Sci. Stat. Comput. **5** (1984), 175–191.

[3] W. J. ELLISON, *A 'Waring's problem' for homogeneous forms.* Proc. Cambridge Philos. Soc. **65** (1969), 663–672.

[4] U. HELMKE, *Waring's problem for binary forms.* J. Pure Appl. Algebra **80** (1992), 29–45.

[5] A. IARROBINO, *Inverse system of a symbolic power II. The Waring problem for forms.* J. Algebra **174** (1995), 1091–1110.

[6] B. F. LOGAN, L. A. SHEPP, *Optimal reconstruction of a function from its projections.* Duke Math. J. **42** (1975), 645–659.

[7] T. MUIR, *A treatise on the theory of determinants.* Dover, 1960.

[8] B. REZNICK, *Sums of powers of complex linear forms*, unpublished manuscript of 1992.

Andrzej SCHINZEL
Institute of Mathematics
Polish Academy of Sciences
00-950 Warsaw
Poland
E-mail : A.Schinzel@impan.gov.pl