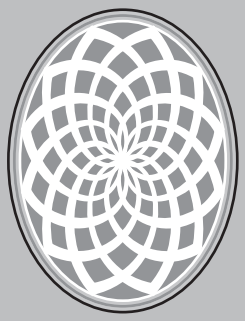

Industrial Mathematics Institute

2000:28

On a decomposition of polynomials in several variables

A. Schinzel

IMI

Preprint Series

Department of Mathematics
University of South Carolina

On a decomposition of polynomials in several variables

by

A. Schinzel (Warszawa)

Dedicated to Michel Mendès France

K. Oskolkov has called my attention to the following theorem used in the theory of polynomial approximation ([2], formula (16)): for every sequence of $d+1$ pairwise linearly independent vectors $[\alpha_{\mu 1}, \alpha_{\mu 2}] \in \mathbb{C}^2$ $(1 \le \mu \le d+1)$ 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 $F \in K[x_1, \dots, x_n]$ there exist polynomials $f_\mu \in K[z]$ $(1 \le \mu \le M)$ such that*

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

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 $M(n, d, K)$ be the least number M such that for every $F \in K[x_1, \dots, x_n]$ of degree d (1) holds for some sequence of vectors $[\alpha_{\mu 1}, \dots, \alpha_{\mu n}] \in K^n$ and some sequence of

polynomials $f_\mu \in K[z]$ $(1 \leq \mu \leq M)$ 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 $\operatorname{char} > d$.*

The problem of determination of $M(n,d,K)$ is related to the problem, much studied in XIX th century (see [3], Lesson XV), of representation of an n-ary form of degree d as the sum of powers of linear forms. The two problems are not equivalent since in our case neither F nor f_μ are supposed homogeneous. Clearly $M(1,d,K) = M(n,1,K) = 1$ and the theorem on reduction of quadratic forms to the diagonal form gives $M(n,2,K) = 2$, provided $\operatorname{char} K \neq 2$.

Theorem 1 gives

$$M(n,d,K) \leq \binom{n+d-1}{n-1}$$

and by counting the constants we obtain

$$M(n,d,K) \geq \frac{1}{n+d-1}\left(\binom{n+d}{n} - 1\right).$$

We shall show

Theorem 2. *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*

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

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

Theorem 3. *For every field K such that*

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

we have

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

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 $K[x_1, \ldots, x_{n-1}]$ of degree at most d in each variable such that $F(a_1, a_2, \ldots, a_{l-1}) = 0$ for all $[a_1, a_2, \ldots, a_{n-1}] \in T_1 \times \ldots \times T_{n-1}$.*

Proof. We proceed by induction on n. For $n = 2$ the statement is immediate. Assume that it is true for polynomials in $n-1$ variables and let

$$F = \sum_{j=0}^{d} F_j(x_1, \ldots, x_{n-1})\, x_n^j$$

satisfy the condition on the degree and

$$F(a_1,\dots,a_n)=0 \text{ for all } [a_1,\dots,a_n]\in T_1\times T_2\times\dots\times T_n.$$

By the case $n=2$ of the lemma

$$F_j(a_1,\dots,a_n)=0 \text{ for all } j\le d \text{ and all } [a_1,\dots,a_{n-1}]\in T_1\times\dots\times T_{n-1}$$

and by the inductive assumption

$$F_j=0 \text{ for all } j\le d,$$

hence $F=0$.

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

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

Define

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

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

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

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

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

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 $A_s = 0 \ \left(1 \le r \le (d+1)^{n-1}\right)$, corresponding to $F = 0$, implies in view of (2) that

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

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

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

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

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

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

Let

$$F\,(x_1, \ldots, x_n) = \sum_{i_1+i_2+\ldots i_n \le d} \begin{pmatrix} i_1 + \ldots + i_n \\ i_1, \ldots, i_n \end{pmatrix} a_{i_1 \ldots i_n} \prod_{j=1}^{n} x_j^{i_j} \tag{6}$$

(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

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

which can be rewritten as

$$\sum_{\mu=1}^{M} b_{\mu l} \prod_{\nu=0}^{n-2} \beta_{\nu,c_\nu(s_\mu)}^{c_\nu(r)} = a_{l - \sum\limits_{\nu=0}^{n-2} c_\nu(r), c_0(r), \ldots, c_{n-2}(r)}$$

$$\left(1 \le r \le (d+1)^{n-1}, \ \sum_{\nu=0}^{n-2} c_\nu(r) \le l\right).$$

By the choice of $s_1, \ldots, s_M$ 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

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

Let us consider

$$F = \begin{cases} x_1 x_2^{p-1} + x_2^d & \text{if } p < d, \\ x_1 x_2^{p-1} & \text{if } p = d. \end{cases}$$

If (1) holds, then

$$x_1 x_2^{p-1} = \sum_{\mu=1}^{\mu} b_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu \right)^p, \ b_\mu \in K,$$

which is clearly impossible.

For the proof of Theorem 2 we need

Lemma 3. *We have the identity*

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

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

Proof. See [1], p. 333.

Proof of Theorem 2. We shall prove first that

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

Applying, if necessary, a linear transformation we may assume that the coefficient of x_1 in $F(x_1, x_2)$ is non-zero. Let then

$$F(x_1, x_2) = \sum_{i_1 + i_2 \leq d} \binom{i_1 + i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2}, \ a_{0d} \neq 0 \tag{8}$$

and let us consider the polynomial

$$G(y_1,\dots,y_{d-2}) = \prod_{1\le i<j\le d-2}(y_j-y_i)\cdot\sum_{i=2}^{d}(-1)^i a_{i,d-i}\tau_{i-2}(y_1,\dots,y_{d-2})$$
$$\cdot\prod_{j=1}^{d-2}\Bigg(-a_{1,d-1}+\sum_{i=2}^{d-1}(-1)^i a_{i,d-i}\left(\tau_{i-1}(y_1,\dots,y_{d-2})+y_j\tau_{i-2}(y_1,\dots,y_{d-2})\right)$$
$$+(-1)^d a_{d,0}y_j\tau_{d-2}(y_1,\dots,y_{d-2})\Bigg).$$

Since $a_{d,0}\neq 0$ the polynomial G is not identically 0 and we have for each $i\le d-2$

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

Since $\operatorname{card} K\ge 2d-2$, 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

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

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

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

However by (10) and Lemma 3

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

Hence the system of equations

$$\sum_{\mu=1}^{d} b_{\mu,l}\beta_\mu^j = a_{l-j,j} \ (0 \le j < l) \tag{12}$$

is solvable for elements $b_{\mu,l}$ of K. We set for $\mu \le d$

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

and obtain (1) from (8), (11) and (12).

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

$$x_1 x_2^{d-1} + a x_2^d = \sum_{\mu=1}^{d-1} f_\mu \left(\alpha_{\mu 1} x_1 + \alpha_{\mu 2} x_2\right). \tag{13}$$

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 (13) 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 (13)

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

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

For the proof of Theorem 3 we need

Lemma 4. *Let $a_1, \dots, a_k$ be distinct elements of $\mathbb{F}_p^*$, $k \ge p-3$. Then*

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

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 $k \geq j \geq 1$ we have the identity

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

hence, by induction

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

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

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

hence, by induction

$$\begin{aligned}\tau_j(a_1, \ldots, a_k) &= (-r)^j - s\tau_{j-1}(a_1, \ldots, a_k) = (-1)^j r^j + (-1)^j s\frac{r^j - s^j}{r-j} \\ &= (-1)^j \frac{r^{j+1} - s^{j+1}}{r-s}.\end{aligned}$$

Proof of Theorem 3. By the last statement in the proof of Theorem 2 we have $M(2, d, K) \geq d$, thus it is remains to prove the reverse inequality. Let

$$F(x_1, x_2) = \sum_{i_1+i_2 \leq d} \binom{i_1+i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \tag{14}$$

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 $t \mapsto f(t) = \sum_{i=0}^{p-1} a_{i,p-1-i} t^i$ is not injective. Then there exist $r, s \in \mathbb{F}_p^*$ such that $r \neq s$ and $f(r) = f(s)$, hence

$$\sum_{i=1}^{p-2} a_{i,p-1-i} \frac{r^i - s^i}{r-s} = 0. \tag{15}$$

Setting $\alpha_{12} = 0$, $\{\alpha_{22}, \ldots, \alpha_{p-2,2}\} = \mathbb{F}_p^* \setminus \{r, s\}$ we have by Lemma 4

$$\begin{aligned}&\tau_i(\alpha_{12}, \ldots, \alpha_{p-2,2}) = \tau_i(\alpha_{22}, \ldots, \alpha_{p-2,2}) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r-s} \ (i \leq p-3), \\ &\tau_{p-2}(\alpha_{12}, \ldots, \alpha_{p-2,2}) = 0,\end{aligned}$$

hence, by (15),

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

and, by Lemma 3,

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

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

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

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-2} b_{\mu,l}\alpha_{\mu 2}^{j} = a_{l-j,j}\ (0\le j<l). \tag{16}$$

for each $l\le p-2$. Then we take

$$f_\mu = \sum_{l=0}^{p-1} b_{\mu,l}z^l\ (0\le\mu\le p-2),\ f_{p-1} = \sum_{l=0}^{p-1} a_{0,l}z^l$$

and obtain from (14) – (16) that

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

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) $a_{p-1,0}\in f\left(\mathbb{F}_p^*\right)$,

(ii) $a_{0,p-1}\in f\left(\mathbb{F}_p^*\right)$,

(iii) $a_{0,p-1}\notin f\left(\mathbb{F}_p^*\right),\ a_{p-1,0}\notin f\left(\mathbb{F}_p^*\right)$.

In the case (i), let

$$a_{p-1,0} = f(r),\ r\in\mathbb{F}_p^*,$$

so that

$$\sum_{i=0}^{p-2} a_{i,p-1-i}r^i = 0. \tag{17}$$

Setting $\alpha_{12}=0$, $\{\alpha_{22},\ldots,\alpha_{p-1,2}\}=\mathbb{F}_p^*\setminus\{r\}$ we have by Lemma 4

$$\tau_i(\alpha_{12},\ldots,\alpha_{p-1,2})=\tau_i(\alpha_{22},\ldots,\alpha_{p-1,2})=(-r)^i (i\le p-2),$$
$$\tau_{p-1}(\alpha_{12},\ldots,\alpha_{p-1,2})=0,$$

hence, by (17),

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

and, by Lemma 3,

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

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

$$\sum_{\mu=1}^{p-1} b_{\mu,p-1}\alpha_{\mu 2}^j=a_{p-1-j,j}\ (0\le j\le p-1). \tag{18}$$

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-1} b_{\mu,l}\alpha_{\mu 2}^j=a_{l-j,j}\ (0\le j\le l). \tag{19}$$

for each $l\le p-2$. Then we take

$$f_\mu=\sum_{l=0}^{p-1} b_{\mu,l}z^l\ (0\le\mu\le p-1)$$

and obtain from (14) and (18) – (16) that

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

In the case (ii), let

$$a_{0,p-1}=f\left(r^{-1}\right),\ r\in\mathbb{F}_p^*,$$

so that

$$\sum_{i=0}^{p-2} a_{p-1-i,i}r^i=\sum_{i=1}^{p-1} a_{i,p-1-i}r^{p-1-i}=0. \tag{20}$$

Setting $\alpha_{11}=0$, $\{\alpha_{21},\dots,\alpha_{p-1,1}\}=\mathbb{F}_p^*\setminus\{r\}$ we have by Lemma 4

$$\tau_i(\alpha_{11},\dots,\alpha_{p-1,1})=\tau_i(\alpha_{21},\dots,\alpha_{p-1,1})=(-r)^i\ (i\le p-2),$$
$$\tau_{p-1}(\alpha_{11},\dots,\alpha_{p-1,1})=0,$$

hence, by (20),

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

and, by Lemma 3,

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

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

$$\sum_{\mu=1}^{p-1} b_{\mu,p-1}\alpha_{\mu 1}^j=a_{j,p-1-j}\ (0\le j\le p-1). \tag{21}$$

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-1} b_{\mu,l}\alpha_{\mu 1}^j=a_{j,l-j}\ (0\le j\le l) \tag{22}$$

for each $l\le p-2$. Then we take

$$f_\mu=\sum_{l=0}^{p-1} b_{\mu,l}z^l\ (0\le\mu\le p-1)$$

and obtain from (14) and (21) – (22)

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

In the case (iii), since

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

we have $a_{p-1,0}=a_{0,p-1}$. Hence the first and the last row of the determinant

$$\begin{vmatrix} 1\dots & 1 & a_{p-1,0}\\ 1\dots & p-1 & a_{p-2,1}\\ \vdots & \vdots & \vdots\\ 1^{p-1}\dots & (p-1)^{p-1} & a_{0,p-1}\end{vmatrix}.$$

are equal and the determinant vanishes.

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

$$\sum_{\mu=1}^{p-1} b_{\mu,p-1}\mu^j = a_{j,p-1-j} \ (0\leq j\leq p-1). \tag{23}$$

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-1} b_{\mu,l}\mu^j = a_{j,l-j} \ (0\leq j\leq l) \tag{24}$$

for each $l\leq p-2$. Then we take

$$f_\mu = \sum_{l=0}^{p-1} b_{\mu,l}z^l \ (0\leq\mu\leq p-1)$$

and obtain from (14) and (23) – (24)

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

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 $t\mapsto f(t)=\sum\limits_{i=0}^{p-2} a_{i,p-2-i}t^i$ is not injective. Then there exist $r,s\in\mathbb{F}_p^*$ such that $r\neq s$ and $f(r)=f(s)$, hence

$$\sum_{i=1}^{p-2} a_{i,p-2-i}\frac{r^i-s^i}{r-s} = 0. \tag{25}$$

Setting $\{\alpha_{12},\ldots,\alpha_{p-3,2}\} = \mathbb{F}_p^*\setminus\{r,s\}$ we have by Lemma 4

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

hence, by (25),

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

and, by Lemma 3,

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

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

$$\sum_{\mu=1}^{p-3} b_{\mu,p-2}\alpha_{\mu 2}^{i} = a_{p-2-j,j}\ (0\le j<p-2). \tag{26}$$

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-3} b_{\mu,l}\alpha_{\mu 2}^{j} = a_{l-j,j}\ (0\le j\le l) \tag{27}$$

for each $l\le p-3$.

Then we take

$$f_\mu = \sum_{l=0}^{p-2} b_{\mu,l}z^l\ (1\le\mu\le p-3),\ f_{p-2} = \sum_{l=0}^{p-2} a_{0,l}z^l$$

and obtain from (14) and (26), (27) that

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

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.

(iv) $$0\in f\left(F_p^*\right),$$

(v) $$0\notin f\left(F_p^*\right).$$

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

$$\sum_{i=0}^{p-2} a_{i,p-2-i}r^i = 0. \tag{28}$$

Setting $\{\alpha_{12},\ldots,\alpha_{p-2,2}\} = \mathbb{F}_p\setminus\{r\}$ we have by Lemma 4

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

hence, by (28)

$$\sum_{i=0}^{p-2}(-1)^i a_{i,p-2-i}\tau_i\left(\alpha_{12},\ldots,\alpha_{p-2,2}\right)=0 \tag{29}$$

and by Lemma 3

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

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

$$\sum_{\mu=1}^{p-2} b_{\mu,p-2}\alpha_{\mu 2}^{j}=a_{p-2-j,j}\ (0\le j\le p-2). \tag{30}$$

We can also solve for $b_{\mu,l}$ in $\mathbb{F}_p$ the system

$$\sum_{\mu=1}^{p-2} b_{\mu,l}\alpha_{\mu 2}^{j}=a_{l-j,j}\ (0\le j\le l) \tag{31}$$

for each $l\le p-3$. Then we take

$$f_\mu=\sum_{l=0}^{p-2} b_{\mu,l}z^l\ (1\le\mu\le p-2)$$

and obtain from (14) and (30) – (31) that

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

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 $rf(r)=sf(s)$:

$$\sum_{i=0}^{p-2} a_{i,p-1-i}\frac{r^{i+1}-s^{i+1}}{r-s}=0. \tag{32}$$

Setting

$$\alpha_{12}=0,\ \{\alpha_{22},\dots,\alpha_{p-1,2}\}=\mathbb{F}_p\setminus\{r,s\}$$

we have by Lemma 4

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

hence, by (32), (29) holds and we conclude the argument as in the case (iv). The proof of Theorem 3 is complete.

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

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

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

$$6b_4+6b_5+18b_6=3,$$
$$6b_4+2b_5+12b_6=2,$$
$$2b_4+6b_5+12b_6=0,$$

which is impossible, since

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

References

[1] T. Muir, *A treatise on the theory of determinants*, Dover 1960.

[2] K. Oskolkov, *Ridge approximation*, Chebyshev-Fourier analysis and quadrature formulas, Proc. Steklov Inst. Math. 219 (1997), 265–280.

[3] G. Salmon, *Lessons introductory to the modern higher algebra*, Chelsea 1964.