Symmetric multilinear forms and polarization of polynomials

Aleš Drápal[a,1], Petr Vojtěchovský[b]

[a] *Department of Algebra, Charles University, Sokolovská 183, Praha 186 75, Czech Republic*

[b] *Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, U.S.A.*

Abstract

We study a generalization of the classical correspondence between homogeneous quadratic polynomials, quadratic forms, and symmetric/alternating bilinear forms to forms in n variables. The main tool is combinatorial polarization, and the approach is applicable even when $n!$ is not invertible in the underlying field.

Key words: n-form, n-application, homogeneous polynomial, quadratic form, n-linear form, characteristic form, polarization, combinatorial polarization

2000 MSC: Primary: 11E76. Secondary: 11E04, 11C08, 05E05.

1. Introduction

Let F be a field of characteristic $\mathrm{char}(F)$, and let V be a d-dimensional vector space over F. Recall that a *quadratic form* $\alpha : V \to F$ is a mapping such that

$$\alpha(au) = a^2\alpha(u) \tag{1.1}$$

for every $a \in F$, $u \in V$, and such that $\varphi : V^2 \to F$ defined by

$$\varphi(u, v) = \alpha(u + v) - \alpha(u) - \alpha(v) \tag{1.2}$$

Email addresses: `drapal@karlin.mff.cuni.cz` (Aleš Drápal), `petr@math.du.edu` (Petr Vojtěchovský)

[1] Supported by institutional grant MSM 0021620839. An early version of this paper was written during Fulbright research stay at the University of Wisconsin-Madison.

is a symmetric bilinear form.

The name "quadratic form" is justified by the fact that quadratic forms $V \to F$ are in one-to-one correspondence with homogeneous quadratic polynomials over F. This is a coincidence, however, and it deserves a careful look:

Assume that $\mathrm{char}(F) \neq 2$. Given a symmetric bilinear form $\varphi : V^2 \to F$, the mapping $\alpha : V \to F$ defined by

$$\alpha(u) = \frac{\varphi(u,u)}{2} \tag{1.3}$$

is clearly a quadratic form satisfying (1.2). Conversely, if α is a quadratic form with associated symmetric bilinear form φ then (1.3) follows, so α can be recovered from φ. Quadratic forms $V \to F$ are therefore in one-to-one correspondence with symmetric bilinear forms $V^2 \to F$. Moreover, upon choosing a basis $\{e_1, \dots, e_d\}$ of V, (1.3) can be rewritten in coordinates as

$$\alpha(\sum_i a_i e_i) = \sum_{i,j} \frac{a_i a_j}{2} \varphi(e_i, e_j),$$

showing that α is indeed a homogeneous quadratic polynomial. Every homogeneous quadratic polynomial is obviously a quadratic form.

Now assume that $\mathrm{char}(F) = 2$. For an alternating bilinear form $\varphi : V^2 \to F$, the homogeneous quadratic polynomial

$$\beta(\sum_i a_i e_i) = \sum_{i<j} a_i a_j \varphi(e_i, e_j) \tag{1.4}$$

satisfies

$$\begin{aligned}\beta(u+v) - \beta(u) - \beta(v) &= \sum_{i<j} (a_i b_j + b_i a_j) \varphi(e_i, e_j) \\ &= \varphi(\sum_i a_i e_i, \sum_j b_j e_j) = \varphi(u,v),\end{aligned}$$

and thus every alternating bilinear form arises in association with some quadratic form. Conversely, if φ is the symmetric bilinear form associated with the quadratic form α, (1.2) implies that φ is alternating. Furthermore, with β as in (1.4), we see that $\gamma = \alpha - \beta$ satisfies $\gamma(u+v) = \gamma(u) + \gamma(v)$. In particular,

$$\gamma(\sum_i a_i e_i) = \sum_i \gamma(a_i e_i) = \sum_i a_i^2 \gamma(e_i),$$

proving that α is a homogeneous quadratic polynomial. Thus we again have the desired correspondence between quadratic forms and homogeneous quadratic polynomials. However, the alternating bilinear form φ associated with α does not determine α uniquely.

The goal of this paper is to investigate generalizations of the three concepts (quadratic form, homogeneous quadratic polynomial and symmetric resp. alternating bilinear form) for any number n of variables, giving rise to polynomial n-applications, a class of polynomials of combinatorial degree $\leq n$, and characteristic n-linear forms, respectively.

The key insight, which goes back at least to Greenberg [5], is the observation that (1.2) is a special case of the so-called *polarization* of α, but many more concepts and observations, most of them new, will be required.

The difficulties encountered with quadratic forms over fields of characteristic two will be analogously encountered for forms in n variables over fields in which $n!$ is not invertible. There are surprises for $n > 3$ (not all n-applications are polynomial) and especially for $n > 4$ (not all polynomial n-applications are homogeneous of degree n).

Finally, we remark that this paper was not written to mindlessly generalize the concept of a quadratic form. Rather, it grew from our need to understand why the prime three behaves differently from all other primes in Richardson's odd code loops [11]. The reason turned out to be the fact that odd code loops are connected to trilinear forms satisfying $\varphi(u, u, u) = 0$. The details of this connection to code loops, and thus indirectly to the Monster group, will be presented separately in a later paper.

2. Polarization, polynomial mappings, and n-applications

In this paper, a *form* is any mapping $V^n \to F$. A form $f : V^n \to F$ is *symmetric* if $f(v_1, \dots, v_n) = f(v_{\sigma(1)}, \dots, v_{\sigma(n)})$ for every $v_1, \dots, v_n \in V$ and every permutation σ of $\{1, \dots, n\}$. A symmetric form $f : V^n \to F$ is *n-additive* if $f(u+w, v_2, \dots, v_n) = f(u, v_2, \dots, v_n) + f(w, v_2, \dots, v_n)$ for every u, w, $v_2, \dots, v_n \in V$, and it is *n-linear* if it is n-additive and $f(av_1, v_2, \dots, v_n) = af(v_1, v_2, \dots, v_n)$ for every $a \in F$, $v_1, \dots, v_n \in V$.

2.1. Polarization

Let $\alpha : V \to F$ be a form satisfying $\alpha(0) = 0$, and let $n \geq 1$. As in Ward [13], the *nth defect* (also called the *nth derived form*) $\Delta^n\alpha : V^n \to F$ of α is defined by

$$\Delta^n\alpha(u_1,\dots,u_n) = \sum_{1\le i_1<\cdots<i_m\le n} (-1)^{n-m}\alpha(u_{i_1}+\cdots+u_{i_m}). \tag{2.1}$$

Then $\Delta^n\alpha$ is clearly a symmetric form, and it is not hard to see, using the inclusion-exclusion principle, that the defining identity (2.1) is equivalent to the recurrence relation

$$\begin{aligned}\Delta^n\alpha(u_1,\dots,u_n) = {} & \Delta^{n-1}\alpha(u_1+u_2,u_3,\dots,u_n) \\ & -\Delta^{n-1}\alpha(u_1,u_3,\dots,u_n) \\ & -\Delta^{n-1}\alpha(u_2,u_3,\dots,u_n).\end{aligned} \tag{2.2}$$

If there is a positive integer n such that $\Delta^n\alpha \neq 0$ and $\Delta^{n+1}\alpha = 0$, we say that α has *combinatorial degree* n, and we write $\mathrm{cdeg}(\alpha) = n$. If α is the zero map, we set $\mathrm{cdeg}(\alpha) = -1$.

Whenever we speak of combinatorial polarization or combinatorial degree of a form $\alpha : V \to F$, we tacitly assume that $\alpha(0) = 0$.

It follows from the recurrence relation (2.2) that $\Delta^m\alpha = 0$ for every $m > \mathrm{cdeg}(\alpha)$. The same relation also shows that $\mathrm{cdeg}(\alpha) = n$ if and only if $\Delta^n\alpha \neq 0$ is a symmetric n-additive form. In particular, when F is a prime field, $\mathrm{cdeg}(\alpha) = n$ if and only if $\Delta^n\alpha \neq 0$ is a symmetric n-linear form.

Note that combinatorial polarization is a linear process, i.e., $\Delta^n(c\alpha + d\beta) = c\Delta^n\alpha + d\Delta^n\beta$ for every c, $d \in F$ and α, $\beta : V \to F$.

In the terminology of Ferrero and Micali [3], a form $\alpha : V \to F$ is an *n-application* if

$$\alpha(au) = a^n\alpha(u) \text{ for every } a \in F,\ u \in V, \text{ and} \tag{2.3}$$

$$\Delta^n\alpha : V^n \to F \text{ is a symmetric } n\text{-linear form.} \tag{2.4}$$

Note that (2.3) and (2.4) are generalizations of (1.1) and (1.2), that is, quadratic forms are precisely 2-applications.

2.2. Polynomial mappings and n-applications

Let $F[x_1,\dots,x_d]$ be the ring of polynomials in variables x_1, …, x_d with coefficients in F. Denote multivariables by $\overline{x} = (x_1,\dots,x_d)$, multiexponents by $\overline{m} = (m_1,\dots,m_d)$, and write $\overline{x}^{\overline{m}}$ instead of $x_1^{m_1}\cdots x_d^{m_d}$. Then every polynomial $f \in F[\overline{x}]$ can be written uniquely as a finite sum of monomials

$$f(\overline{x}) = \sum c(\overline{m})\overline{x}^{\overline{m}},$$

where $c(\overline{m}) \in F$ for every multiexponent $\overline{m}$. Finally, let $M(f) = \{\overline{m};\ c(\overline{m}) \neq 0\}$ be the set of all multiexponents of f.

The *degree of* $f \in F[\overline{x}]$ is $\deg(f) = \max\{m_1 + \cdots + m_d;\ (m_1, \ldots, m_d) \in M(f)\}$.

Define a binary relation $\sim$ on $F[\overline{x}]$ as follows: For a variable x_i and exponents m_i, n_i let $x_i^{m_i} \sim x_i^{n_i}$ if and only if either $m_i = n_i$, or $m_i > 0$, $n_i > 0$ and $m_i - n_i$ is a multiple of $|F| - 1$. (When F is infinite, $m_i - n_i$ is a multiple of $|F| - 1$ if and only if $m_i = n_i$.) Then let $c(\overline{m})\overline{x}^{\overline{m}} \sim c(\overline{n})\overline{x}^{\overline{n}}$ if and only if $c(\overline{m}) = c(\overline{n})$ and $x_i^{m_i} \sim x_i^{n_i}$ for every $1 \leq i \leq d$. It is not difficult to see that $\sim$ extends linearly into an equivalence on $F[\overline{x}]$.

We call $F[\overline{x}]/\!\sim$ *reduced polynomials*. Given a polynomial $f \in F[\overline{x}]$, the equivalence class $[f]_\sim$ contains a unique polynomial g such that $0 \leq m_i < |F|$ for every $1 \leq i \leq d$, $\overline{m} \in M(g)$. We usually identify $[f]_\sim$ with this representative g, and refer to g as a reduced polynomial, too.

The significance of reduced polynomials rests in the fact that they are precisely the polynomial functions:

Lemma 2.1. *Let f, $g \in F[\overline{x}]$. Then $[f]_\sim = [g]_\sim$ if and only if $f - g$ is the zero function.*

Let $\alpha : V \to F$ be a mapping and $B = \{e_1, \ldots, e_d\}$ a basis of V. Then α is a *polynomial mapping with respect to B* if there exists a polynomial $f \in F[\overline{x}]$ such that

$$\alpha(\sum_i a_i e_i) = f(a_1, \ldots, a_d)$$

for every a_1, $\ldots$, $a_d \in F$. We say that f *realizes α with respect to B*. By Lemma 2.1, there is a unique reduced polynomial realizing α with respect to B.

A change of basis will result in a different polynomial representative for a polynomial mapping, but many properties of the representative remain intact.

Lemma 2.2. *Let $\alpha : V \to F$ be realized with respect to a basis B of V by some reduced polynomial $f \in F[\overline{x}]$. If B^* is another basis of V then α is realized by some reduced polynomial $f^* \in F[\overline{x}]$ with respect to B^* and* $\deg(f) = \deg(f^*)$.

Proof. Let $B = \{e_1, \dots, e_d\}$, $B^* = \{e_1^*, \dots, e_d^*\}$, $e_i^* = \sum_j c_{i,j} e_j$. Then

$$\begin{aligned}\alpha\big(\sum_i a_i e_i^*\big) &= \alpha\big(\sum_i a_i \sum_j c_{i,j} e_j\big)\\ &= \alpha\big(\sum_j \big(\sum_i a_i c_{i,j}\big) e_j\big) = f\big(\sum_i a_i c_{i,1}, \dots, \sum_i a_i c_{i,d}\big),\end{aligned}$$

which is some polynomial f^* in $a_1, \dots, a_d$.

We clearly have $\deg(f) = \deg(f^*)$ when $e_1^* = ce_1$ for some $c \neq 0$ and $e_i^* = e_i$ for every $i > 1$. We can therefore assume that $e_1^* = e_1 + e_2$ and $e_i^* = e_i$ for every $i > 1$. (Every change of basis is a product of these two types of elementary operations.)

Let $g(\overline{x}) = \overline{x}^{\overline{m}}$ be a monomial of f such that $\deg(g) = \deg(f)$. Then

$$g\big(\sum_i x_i c_{i,1}, \dots, \sum_i x_i c_{i,d}\big) = (x_1 + x_2)^{m_1} x_2^{m_2} \cdots x_d^{m_d} \tag{2.5}$$

contains the reduced monomial $g(\overline{x})$ as a summand that cannot be cancelled with any other summand of (2.5), nor any other summand of f^*, due to $\deg(g) = \deg(f)$. This means that $\deg(f^*) \geq \deg(g) = \deg(f)$, and the other inequality follows by symmetry. □

We say that a mapping $\alpha : V \to F$ is a *polynomial mapping of degree* n if α is realized by a reduced polynomial of degree n with respect to some (and hence every) basis of V.

We have seen in the Introduction that every 2-application is a polynomial mapping, in fact a homogeneous quadratic polynomial. It is a fascinating question whether every n-application is a polynomial mapping, and the series of papers [6]–[10] by Prószyński is devoted to this question, albeit in the more general setting of mappings between modules.

Of course, every n-application $V \to F$ is a polynomial mapping when F is finite, since any mapping $V \to F$ is then a polynomial by Lagrange's Interpolation. Prószynski proved that any 3-application is a polynomial mapping [6, Theorem 4.4], and showed after substantial effort that for every $n > 3$ there is an n-application over a field of characteristic two that is not a polynomial mapping [9, Example 4.5].

For $n > 3$, there is therefore no hope of maintaining the correspondence between n-applications and a certain class of polynomials, unless we restrict our attention to polynomial n-applications.

We present a characterization of polynomials that are n-applications in Section 5. But first we have a look at forms obtained by polarization.

3. Characteristic forms

For all fields F containing the rational numbers, we will find it convenient to set $\mathrm{char}(F) = \infty$, rather than the more contemporary $\mathrm{char}(F) = 0$.

Since we will often deal with repeated arguments, we adopt the following notation from multisets, cf. [1]: For an integer r and a vector u, we understand by $r * u$ that u is used r times. For instance, $\varphi(r * u, s * v)$ stands for

$$\varphi(\underbrace{u, \quad \ldots, \quad u}_{r \text{ times}}, \underbrace{v, \quad \ldots, \quad v}_{s \text{ times}}).$$

With these conventions in place, a symmetric form $\varphi : V^n \to F$ is said to be *characteristic* if either $n < \mathrm{char}(F)$, or $n \geq \mathrm{char}(F) = p$ and $\varphi(p * u, v_1, \ldots, v_{n-p}) = 0$ for every u, v_1, …, $v_{n-p} \in V$. Note that every symmetric form in characteristic ∞ is characteristic.

All forms arising by polarization are characteristic:

Lemma 3.1. *Let $\alpha : V \to F$ and $n \geq 1$. Then $\Delta^n \alpha : V^n \to F$ is a characteristic form.*

Proof. There is nothing to prove when $n < \mathrm{char}(F)$. Assume that $n \geq p = \mathrm{char}(F)$ and let u, v_1, …, $v_{n-p} \in V$. By definition of $\Delta^n \alpha$,

$$\Delta^n \alpha(p * u, v_1, \ldots, v_{n-p}) = \sum \sum_{k=0}^{p} (-1)^{n-r-k} \binom{p}{k} \alpha(ku + v_{i_1} + \cdots + v_{i_r}),$$

where the outer summation runs over all subsets $\{i_1, \ldots, i_r\}$ of $\{1, \ldots, n-p\}$. Since p divides $\binom{p}{k}$ unless $k = 0$ or $k = p$, the inner sum reduces to

$$(-1)^{n-r} \alpha(v_{i_1} + \cdots + v_{i_r}) + (-1)^{n-r-p} \alpha(v_{i_1} + \cdots + v_{i_r}).$$

When p is odd, the two signs $(-1)^{n-r}$ and $(-1)^{n-r-p}$ are opposite to each other, and the inner sum vanishes. When p is even, the two signs are the same and the inner sum becomes $2\alpha(v_{i_1} + \cdots + v_{i_r}) = 0$. □

In the rest of this section we show that: (a) every characteristic n-additive form can be realized by polarization if $n!$ is invertible, and (b) every characteristic n-linear form can be realized by polarization of a homogeneous polynomial of degree n with all exponents less than $\mathrm{char}(F)$. For (a), we generalize (1.3) and set

$$\alpha(u) = \frac{\varphi(n * u)}{n!}.$$

For (b), we generalize (1.4), once again having to resort to coordinates.

Result (a) is mentioned without proof by Greenberg [5, p. 110] and it has been rediscovered and proved by Ferrero and Micali in [3]. To our knowledge, (b) is new.

Lemma 3.2. *Let φ, $\psi : V^n \to F$ be characteristic n-additive forms such that*

$$\varphi(u_1, \dots, u_n) = \psi(u_1, \dots, u_n)$$

whenever u_1, ..., u_n are pairwise distinct vectors of V. Then $\varphi = \psi$.

Proof. Assume that $\varphi(s_1 * u_1, \dots, s_m * u_m) \neq \psi(s_1 * u_1, \dots, s_m * u_m)$ for some pairwise distinct vectors u_1, ..., u_m and positive integers s_1, ..., s_m, where $s_1 + \cdots + s_m = n$ and where m is as small as possible. Note that $u_i \neq 0$ for every i by additivity, and $s_i < \mathrm{char}(F)$ since both φ, ψ are characteristic.

Suppose for a while that $u_2 = ku_1$ for an integer $0 < k < \mathrm{char}(F)$. Then

$$\begin{aligned} k^{s_2}\varphi(s_1 * u_1, s_2 * u_1, s_3 * u_3, \dots, s_m * u_m) &= \varphi(s_1 * u_1, s_2 * u_2, \dots, s_m * u_m) \\ \neq \psi(s_1 * u_1, s_2 * u_2, \dots, s_m * u_m) &= k^{s_2}\psi(s_1 * u_1, s_2 * u_1, s_3 * u_3, \dots, s_m * u_m) \end{aligned}$$

and thus

$$\varphi((s_1 + s_2) * u_1, s_3 * u_3, \dots, s_m * u_m) \neq \psi((s_1 + s_2) * u_1, s_3 * u_3, \dots, s_m * u_m),$$

a contradiction with minimality of m.

We can therefore assume that for every $i \neq j$ and every $0 < k < \mathrm{char}(F)$ we have $u_i \neq ku_j$. Then $v_1 = u_1$, $v_2 = 2u_1$, ..., $v_{s_1} = s_1u_1$, $v_{s_1+1} = u_2$, ..., $v_{s_1+s_2} = s_2u_2$, ..., $v_n = s_mu_m$ are n distinct vectors and

$$\varphi(v_1, \dots, v_n) = \varphi(s_1 * u_1, \dots, s_m * u_m)\prod_{i=1}^{m} s_i!$$

is not equal to

$$\psi(s_1 * u_1, \dots, s_m * u_m) \prod_{i=1}^{m} s_i! = \psi(v_1, \dots, v_n),$$

a contradiction. $\square$

Proposition 3.3. *Let $n < \mathrm{char}(F)$, and let $\varphi : V^n \to F$ be a characteristic n-additive form. Then $\alpha : V \to F$ defined by*

$$\alpha(u) = \frac{\varphi(n * u)}{n!}$$

satisfies $\Delta^n \alpha = \varphi$.

Proof. Both $\Delta^n \alpha$ and φ are characteristic since $n < \mathrm{char}(F)$. By Lemma 3.2, it suffices to show that $\Delta^n \alpha(u_1, \dots, u_n) = \varphi(u_1, \dots, u_n)$ for every pairwise distinct vectors $u_1, \dots, u_n$ of V. We have

$$\begin{aligned} \Delta^n \alpha(u_1, \dots, u_n) &= \sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^{n-k} \alpha(u_{i_1} + \cdots + u_{i_k}) \\ &= \frac{1}{n!} \sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^{n-k} \varphi(n * (u_{i_1} + \cdots + u_{i_k})). \end{aligned}$$

Let $v_1, \dots, v_m$ be pairwise distinct vectors of V such that $v_1, \dots, v_m \in \{u_1, \dots, u_n\}$, and let $1 \le s_i \le n$ be such that $s_1 + \cdots + s_m = n$. We count how many times $\varphi(s_1 * v_1, \dots, s_m * v_m)$ appears in $\Delta^n \alpha(u_1, \dots, u_n)$. It appears precisely in those summands $\varphi(n * (u_{i_1} + \cdots + u_{i_k}))$ satisfying $\{v_1, \dots, v_m\} \subseteq \{u_{i_1}, \dots, u_{i_k}\}$, and then it appears

$$\binom{n}{s_1, \dots, s_m} = \frac{n!}{s_1! \cdots s_m!}$$

times; a number that is independent of k. For a fixed ℓ, there are precisely $\binom{n-m}{\ell}$ subsets $\{u_{i_1}, \dots, u_{i_{\ell+m}}\}$ containing $\{v_1, \dots, v_m\}$. Altogether, $\varphi(s_1 * v_1, \dots, s_m * v_m)$ appears with multiplicity

$$\binom{n}{s_1, \dots, s_m} \sum_{\ell=0}^{n-m} (-1)^{n-(\ell+m)} \binom{n-m}{\ell}. \tag{3.1}$$

Recall that

$$\sum_{\ell=0}^{n}(-1)^{\ell}\binom{n}{\ell} = \begin{cases} 1, & n=0, \\ 0, & n>0. \end{cases}$$

Hence (3.1) vanishes when $m < n$. When $m = n$, we have $s_1 = \cdots = s_n = 1$, and so (3.1) is equal to $n!$. □

Theorem 3.4 (Realizing characteristic n-linear forms by polarization)**.** *Let $\{e_1, \ldots, e_d\}$ be a basis of V and let $\varphi : V^n \to F$ be a characteristic n-linear form. Define $\alpha : V \to F$ by*

$$\alpha(\sum a_i e_i) = \sum_{\substack{t_1+\cdots+t_d=n \\ 0\le t_i<\mathrm{char}(F)}} \frac{a_1^{t_1}\cdots a_d^{t_d}}{t_1!\cdots t_d!}\varphi(t_1 * e_1, \ldots, t_d * e_d). \tag{3.2}$$

Then $\Delta^n\alpha = \varphi$. Moreover, α is a homogeneous polynomial of degree n with all exponents less than $\mathrm{char}(F)$*.*

Proof. Let $p = \mathrm{char}(F) \le \infty$. By n-linearity and symmetry of φ, we have

$$\varphi\left(n * \sum_{i=1}^{d} a_i e_i\right) = \sum_{\substack{t_1+\cdots+t_d=n \\ 0\le t_i\le n}} \binom{n}{t_1, \ldots, t_d} a_1^{t_1}\cdots a_d^{t_d}\varphi(t_1 * e_1, \ldots, t_d * e_d).$$

Since φ is characteristic, we can rewrite this as

$$\varphi\left(n* \sum_{i=1}^{d} a_i e_i\right) = \sum_{\substack{t_1+\cdots+t_d=n \\ 0\le t_i<p}} \binom{n}{t_1, \ldots, t_d} a_1^{t_1}\cdots a_d^{t_d}\varphi(t_1 * e_1, \ldots, t_d * e_d). \tag{3.3}$$

If $n < p$, we can divide (3.3) by $n!$ and apply Proposition 3.3. For the rest of the proof assume that $n \ge p$.

Then all summands of the right hand side of (3.3) vanish, since the multinomial coefficients $\binom{n}{t_1,\ldots,t_d}$ are equal to zero (as $t_i < p$). In fact, the multiplicity of p in the prime factorization of $\binom{n}{t_1,\ldots,t_d}$, say p^m, is the same as the multiplicity of p in the prime factorization of $n!$. Thus, upon formally dividing (3.3) by $n!$, the left hand side of (3.3) becomes $\varphi(n * u)/n!$ and the right hand side of (3.3) becomes $\alpha(u)$. The calculation in the proof of Proposition 3.3 therefore still applies, proving $\Delta^n\alpha = \varphi$.

Finally, α is obviously a homogeneous polynomial of degree n with all exponents less than $\mathrm{char}(F)$. □

Example 3.5 ($n = p = 3$)**.** *Let $\varphi : V^3 \to \mathbb{F}_3$ be a characteristic trilinear form. Let $\{e_1, e_2, e_3\}$ be a basis of V, and $u = a_1e_1 + a_2e_2 + a_3e_3$. Then*

$$\varphi(u, u, u) = \sum_{i \neq j} 3a_i^2 a_j \varphi(e_i, e_i, e_j) + \sum_{i<j<k} 6a_i a_j a_k \varphi(e_i, e_j, e_k).$$

Upon formally dividing this equality by $3!$*, we obtain the homogeneous polynomial from Theorem 3.4, namely*

$$\alpha(u) = \sum_{i \neq j} \frac{a_i^2 a_j}{2} \varphi(e_i, e_i, e_j) + \sum_{i<j<k} a_i a_j a_k \varphi(e_i, e_j, e_k).$$

A careful reader might wonder if the property that every exponent is less than $\mathrm{char}(F)$ is invariant under a change of basis. In general the answer is "no", but for mappings of the form (3.2) the answer is "yes", see Lemma 5.2.

4. Combinatorial degree of polynomial mappings

We now wish to return to the question: *Which polynomial mappings are n-applications?* Our task is therefore to characterize polynomial mappings α that satisfy the homogeneity condition $\alpha(au) = a^n\alpha(u)$ and for which $\Delta^n\alpha$ is n-linear. When F is a prime field, $\Delta^n\alpha$ is n-linear if and only if $\Delta^n\alpha$ is n-additive, which happens if and only if $\mathrm{cdeg}(\alpha) \leq n$. We therefore need to know how to calculate the combinatorial degree of polynomial mappings, which is what we are going to explain in this section. In the next section, we tackle the homogeneity condition and the linearity of $\Delta^n\alpha$ with respect to scalar multiplication.

Let t be a nonnegative integer and p a prime, where we also allow $p = \infty$. Then there are uniquely determined integers t_i, the *p-adic digits of t*, satisfying $0 \leq t_i < p$ and $t = t_0p^0 + t_1p^1 + t_2p^2 + \cdots$. In particular, when $p = \infty$, then $t_0 = t$ and $t_i = 0$ for $i > 0$, using the convention $\infty^0 = 1$. The *p-weight $\omega_p(t)$ of t* is the sum $t_0 + t_1 + t_2 + \cdots$.

Let $p = \mathrm{char}(F)$. The *p-degree of a monomial $\overline{x}^{\overline{m}}$* $\in F[\overline{x}]$ is

$$\deg_p(\overline{x}^{\overline{m}}) = \sum_{i=1}^{d} \omega_p(m_i),$$

and the *p-degree of a polynomial f* $\in F[\overline{x}]$ is

$$\deg_p(f) = \max\{\deg_p(\overline{x}^{\overline{m}});\ \overline{m} \in M(f)\}.$$

In particular, when $p = \infty$, $\deg_p(f) = \deg(f)$.

In [13], Ward showed:

Proposition 4.1. *Let F be a prime field or a field of characteristic ∞, V a vector space over F, and $\alpha : V \to F$ a polynomial mapping satisfying $\alpha(0) = 0$. Then* $\operatorname{cdeg}(\alpha) = \deg(\alpha)$.

He also mentioned [13, p. 195] that "It is not difficult to show that, in general, the combinatorial degree of a [reduced] nonzero polynomial over $\mathbb{F}_q$, q a power of the prime p, is the largest value of the sum of the p-weights of the exponents for the monomials appearing in the polynomial." A proof of this assertion can be found already in [12]. Here we prove a more general result for polynomials over any field, not just for polynomials over finite fields $\mathbb{F}_q$. We follow the technique of [12] very closely.

When $\overline{x_1} = (x_{1,1}, \dots, x_{1,d})$, $\overline{x_2} = (x_{2,1}, \dots, x_{2,d})$ are two multivariables, we write $\overline{x_1} + \overline{x_2}$ for the multivariable $(x_{1,1} + x_{2,1}, \dots, x_{1,d} + x_{2,d})$. Moreover, when $\overline{m} = (m_1, \dots, m_d)$ is a multiexponent, we write $(\overline{x_1} + \overline{x_2})^{\overline{m}}$ for $(x_{1,1} + x_{2,1})^{m_1} \cdots (x_{1,d} + x_{2,d})^{m_d}$. For $f \in F[\overline{x}]$ satisfying $f(0) = 0$ and for $n \geq 1$ let $\Delta^n f \in F[x_{1,1}, \dots, x_{1,d}, \dots, x_{n,1}, \dots, x_{n,d}]$ be defined by

$$\Delta^n f(\overline{x_1}, \dots, \overline{x_n}) = \sum_{1 \leq i_1 < \cdots < i_m \leq n} (-1)^{n-m} f(\overline{x_{i_1}} + \cdots + \overline{x_{i_m}}). \tag{4.1}$$

The *(formal) combinatorial degree* $\operatorname{cdeg}(f)$ *of* $f \in F[\overline{x}]$ is the least integer n such that $\Delta^n f$ is a nonzero polynomial and $\Delta^{n+1} f$ is the zero polynomial, letting again $\operatorname{cdeg}(0) = -1$.

Whenever we speak of combinatorial polarization or combinatorial degree of a polynomial f, we tacitly assume that $f(0) = 0$.

We shall show in Theorem 4.8 that $\operatorname{cdeg}(f) = \deg_p(f)$ for every $f \in F[\overline{x}]$ and in Corollary 4.11 that $\operatorname{cdeg}(\alpha) = \operatorname{cdeg}(f)$ whenever $\alpha : V \to F$ is a polynomial mapping realized by f with respect to some basis of V.

Lemma 4.2. *If f, $g \in F[\overline{x}]$ satisfy $M(f) \cap M(g) = \emptyset$ then $M(\Delta^n f) \cap M(\Delta^n g) = \emptyset$ for every $n \geq 1$.*

Proof. It suffices to establish the lemma when f, g are monomials, since combinatorial polarization is a linear process. Let $f(\overline{x}) = \overline{x}^{\overline{m}}$. Consider one of the summands $f(\overline{x_1} + \cdots + \overline{x_s})$ of $\Delta^n f(\overline{x_1}, \dots, \overline{x_n})$, as displayed in (4.1). We have

$$f(\overline{x_1} + \cdots + \overline{x_s}) = (\overline{x_1} + \cdots + \overline{x_s})^{\overline{m}} = (x_{1,1} + \cdots + x_{s,1})^{m_1} \cdots (x_{1,d} + \cdots + x_{s,d})^{m_d}.$$

In turn, let h be a summand of $f(\overline{x_1}+\cdots+\overline{x_s})$. By the multinomial theorem, for every $1 \le i \le d$, the variables $x_{1,i}, \ldots, x_{s,i}$ appear in h precisely m_i times, counting multiplicities. Hence the multiexponent $\overline{m}$ can be reconstructed from any monomial of $\Delta^n f(\overline{x_1}, \ldots, \overline{x_n})$. $\square$

Corollary 4.3. *Assume that $f \in F[\overline{x}]$ satisfies $f(0) = 0$. Then* $\operatorname{cdeg}(f) = \max\{\operatorname{cdeg}(\overline{x}^{\overline{m}});\ \overline{m} \in M(f)\}$.

We proceed to determine the combinatorial degree of monomials.

Let $\overline{m}$, $\overline{n}$ be two multiexponents. We write $\overline{m} \le \overline{n}$ if $m_i \le n_i$ for every $1 \le i \le d$. When $\overline{m} \le \overline{n}$, $\overline{n} - \overline{m}$ stands for the multiexponent $(n_1 - m_1, \ldots, n_d - m_d)$. We also let

$$\binom{\overline{m}}{\overline{n}} = \prod_{i=1}^{d} \binom{m_i}{n_i} = \prod_{i=1}^{d} \frac{m_i!}{n_i!(m_i - n_i)!},$$

with the usual convention $0! = 1$.

The following lemma gives a critical insight into defects of monomials.

Lemma 4.4. *Let $f(\overline{x}) = \overline{x}^{\overline{m}} \in F[\overline{x}]$. Let $\overline{x_1}, \ldots, \overline{x_s}$ be multivariables. Then*

$$\Delta^s f(\overline{x_1}, \ldots, \overline{x_s}) = \sum \binom{\overline{m_1}}{\overline{m_2}} \cdots \binom{\overline{m_{s-1}}}{\overline{m_s}} \overline{x_1}^{\overline{m_s}} \overline{x_2}^{\overline{m_{s-1}}-\overline{m_s}} \cdots \overline{x_s}^{\overline{m_1}-\overline{m_2}}, \quad (4.2)$$

where the summation ranges over all chains of multiexponents $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$.

Proof. Straightforward calculation shows that

$$(\overline{x} + \overline{y})^{\overline{m}} = \prod_{i=1}^{d} (x_i + y_i)^{m_i} = \prod_{i=1}^{d} \sum_{n_i=0}^{m_i} \binom{m_i}{n_i} x_i^{n_i} y_i^{m_i - n_i}$$

is equal to

$$\sum_{0 \le \overline{n} \le \overline{m}} \prod_{i=1}^{d} \binom{m_i}{n_i} x_1^{n_1} \cdots x_d^{n_d} y_1^{m_1 - n_1} \cdots y_d^{m_d - n_d} = \sum_{0 \le \overline{n} \le \overline{m}} \binom{\overline{m}}{\overline{n}} \overline{x}^{\overline{n}} \overline{y}^{\overline{m} - \overline{n}}.$$

Since $\Delta^2 f(\overline{x}, \overline{y}) = (\overline{x} + \overline{y})^{\overline{m}} - \overline{x}^{\overline{m}} - \overline{y}^{\overline{m}}$, the lemma follows for $s = 2$.

Assume that the lemma holds for $s \geq 2$. Let $g_{\overline{m_s}}(\overline{x}) = \overline{x}^{\overline{m_s}}$ and note that we have just proved

$$\Delta^2 g_{\overline{m_s}}(\overline{x_1}, \overline{x_2}) = \sum_{0 < \overline{m_{s+1}} < \overline{m_s}} \binom{\overline{m_s}}{\overline{m_{s+1}}} \overline{x_1}^{\overline{m_{s+1}}} \overline{x_2}^{\overline{m_s} - \overline{m_{s+1}}}. \tag{4.3}$$

Using an analogy of (2.2) for formal polynomials and the induction assumption, we have

$$\begin{aligned}
&\Delta^{s+1} f(\overline{x_1}, \ldots, \overline{x_{s+1}}) \\
&= \Delta^s f(\overline{x_1} + \overline{x_2}, \overline{x_3}, \ldots, \overline{x_{s+1}}) - \Delta^s f(\overline{x_1}, \overline{x_3}, \ldots, \overline{x_{s+1}}) - \Delta^s f(\overline{x_2}, \overline{x_3}, \ldots, \overline{x_{s+1}}) \\
&= \sum \binom{\overline{m_1}}{\overline{m_2}} \cdots \binom{\overline{m_{s-1}}}{\overline{m_s}} ((\overline{x_1} + \overline{x_2})^{\overline{m_s}} - \overline{x_1}^{\overline{m_s}} - \overline{x_2}^{\overline{m_s}}) \overline{x_3}^{\overline{m_{s-1}} - \overline{m_s}} \cdots \overline{x_{s+1}}^{\overline{m_1} - \overline{m_2}} \\
&= \sum \binom{\overline{m_1}}{\overline{m_2}} \cdots \binom{\overline{m_{s-1}}}{\overline{m_s}} \Delta^2 g_{\overline{m_s}}(\overline{x_1}, \overline{x_2}) \overline{x_3}^{\overline{m_{s-1}} - \overline{m_s}} \cdots \overline{x_{s+1}}^{\overline{m_1} - \overline{m_2}},
\end{aligned}$$

where the summation ranges over all chains of multiexponents $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$. We are done upon substituting (4.3) into the last equation. $\square$

Note that the multiexponents of $\overline{x_1}$, $\overline{x_2}$, $\cdots$, $\overline{x_s}$ in the sum of (4.2) are different for every chain $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$. Therefore, by Lemma 4.2, the combinatorial degree of $\overline{x}^{\overline{m}}$ is the length s of a longest chain $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$ satisfying

$$\binom{\overline{m_i}}{\overline{m_{i+1}}} \neq 0 \tag{4.4}$$

for every $1 \leq i < s$, where the inequality is understood in F.

Let us call a chain $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$ of multiexponents satisfying (4.4) *regular*.

Lemma 4.5. *Let $n = \sum_{i=0}^{\infty} n_i p^i$, where $0 \leq n_i < p$ for every i. Then the length of a longest regular chain for $\overline{m} = (n)$ is $\omega_p(n)$.*

Proof. There is nothing to prove in characteristic $p = \infty$. Assume that $p < \infty$, and let $a = \sum_{i=0}^{\infty} a_i p^i$, $b = \sum_{i=0}^{\infty} b_i p^i$ be two integers with $0 \leq a_i$, $b_i < p$ for every i. By Lucas Theorem [4],

$$\binom{a}{b} \equiv \prod_{i=0}^{\infty} \binom{a_i}{b_i}$$

modulo p. Consequently, if $\binom{a}{b} \not\equiv 0$, we must have $a_i \geq b_i$ for every i since $\binom{a_i}{b_i}$ is not divisible by p.

Hence the length t of a longest regular chain for n cannot exceed $\omega_p(n) = \sum_{i=0}^{\infty} n_i$. On the other hand, $t \geq \omega_p(n)$ holds, because we can construct a regular chain for n of length $\omega_p(n)$ by reducing one of the n_is by one in each step. $\square$

Lemma 4.6. *Let $\overline{m} = (m_1, \ldots, m_d)$ be a multiexponent. Let $\overline{m} = \overline{m_1} > \overline{m_2} > \cdots > \overline{m_s} > \overline{0}$ be a longest regular chain for $\overline{m}$. Then $\overline{m_i}$, $\overline{m_{i+1}}$ differ in exactly one exponent for every $1 \leq i < s$, and $s = \sum_{i=1}^{d} \omega_p(m_i)$, where $p = \mathrm{char}(F) \leq \infty$.*

Proof. If $\overline{m_i}$, $\overline{m_{i+1}}$ differ in two exponents, we can construct a longer regular chain by reducing the powers separately. Thus, given the regular chain $\overline{m} = \overline{m_1} > \cdots > \overline{m_s} > \overline{0}$, we can construct another regular chain for $\overline{m}$ of length s, in which we first reduce only the first exponent, then the second exponent, etc. We are done by Lemma 4.5. $\square$

Example 4.7. *Let us construct a longest regular chain for $(7, 4)$ in characteristic $p = 3$. Since $7 = 1 \cdot 3^0 + 2 \cdot 3^1$ and $4 = 1 \cdot 3^0 + 1 \cdot 3^1$, the procedure outlined in the proof of Lemma 4.6 yields the chain $(7, 4) > (4, 4) > (1, 4) > (0, 4) > (0, 1) > (0, 0)$, for instance. The chain has length $5 = \omega_3(7) + \omega_3(4)$, as expected.*

We summarize Corollary 4.3 and Lemmas 4.4, 4.6:

Theorem 4.8 (Combinatorial degree of formal polynomials)**.** *Let $f \in F[\overline{x}]$ be a polynomial satisfying $f(0) = 0$, and let $\mathrm{char}(F) = p \leq \infty$. Then $\mathrm{cdeg}(f) = \deg_p(f)$.*

We now return to combinatorial polarization of polynomial mappings. First observe:

Lemma 4.9. *Let $f \in F[\overline{x}]$ be a reduced polynomial satisfying $f(0) = 0$. Then $\Delta^n f \in F[\overline{x_1}, \ldots, \overline{x_n}]$ is a reduced polynomial for every $n \geq 1$.*

Lemma 4.10. *Let $\alpha : V \to F$ be a polynomial mapping satisfying $\alpha(0) = 0$, and assume that the reduced polynomial $f \in F[\overline{x}]$ represents α with respect to some basis of V. Then $\mathrm{cdeg}(f) = \mathrm{cdeg}(\alpha)$.*

Proof. Let $\{e_1, \ldots, e_d\}$ be the underlying basis. Let $n \geq 1$, and $u_i = \sum_j a_{ij}e_j$. Then

$$\begin{aligned}\Delta^n\alpha(u_1, \ldots, u_n) = \alpha\big(\sum_j a_{1j}e_1, \ldots, \sum_j a_{nj}e_j\big)\\ = \Delta^n f(a_{11}, \ldots, a_{1d}, \ldots, a_{n1}, \ldots, a_{nd}).\end{aligned} \tag{4.5}$$

This equality implies $\mathrm{cdeg}(f) \geq \mathrm{cdeg}(\alpha)$, since if $\Delta^n\alpha \neq 0$ then $\Delta^n f$ is a nonzero function and thus a nonzero polynomial.

On the other hand, assume that $n = \mathrm{cdeg}(f)$. Then $\Delta^n f$ is a nonzero polynomial that is reduced by Lemma 4.9. Thus $\Delta^n f$ is a nonzero function by Lemma 2.1, and (4.5) implies that $\mathrm{cdeg}(\alpha) \geq n = \mathrm{cdeg}(f)$. □

Corollary 4.11 (Combinatorial degree of polynomial mappings)**.** *Let V be a vector space over a field F of characteristic $p \leq \infty$, and let $\alpha : V \to F$ be a nonzero polynomial mapping satisfying $\alpha(0) = 0$. Then* $\mathrm{cdeg}(\alpha)$ *is equal to* $\deg_p(f)$*, where $f \in F[x_1, \ldots, x_d]$ is a reduced polynomial that realizes α with respect to some basis of V.*

5. Polynomial *n*-applications

5.1. Totally reduced polynomials

We have already established that the degree of a polynomial mapping is well-defined, cf. Lemma 2.2. By Corollary 4.11, the combinatorial degree is also well-defined for polynomial mappings.

However, one has to be careful with even the most common concepts, such as the property of being homogeneous. To wit, consider the polynomial mapping $\alpha : \mathbb{F}_4^2 \to \mathbb{F}_4$ defined by $\alpha(a_1e_1 + a_2e_2) = a_1^2a_2^2$ with respect to some basis $\{e_1, e_2\}$ of $\mathbb{F}_4^2$ over $\mathbb{F}_4$. Then

$$\begin{aligned}\alpha(a_1(e_1 + e_2) + a_2e_2) = \alpha(a_1e_1 + (a_1 + a_2)e_2) =\\ a_1^2(a_1 + a_2)^2 = a_1^4 + a_1^2a_2^2 = a_1 + a_1^2a_2^2.\end{aligned}$$

Thus, as a reduced polynomial, α is homogeneous with respect to $\{e_1, e_2\}$ but not with respect to $\{e_1 + e_2, e_2\}$. Of course, no difficulties arise with respect to homogeneity if we do not insist that polynomials be reduced.

Let us consider another property of polynomials familiar to us from Theorem 3.4: A polynomial $f \in F[x_1, \ldots, x_d]$ is *totally reduced* if for every $\overline{m} \in M(f)$ and every $1 \leq i \leq d$ we have $0 \leq m_i < \mathrm{char}(F)$.

Theorem 4.8 implies immediately:

Corollary 5.1. *Let $f \in F[\overline{x}]$ be a monomial. Then $\mathrm{cdeg}(f) \leq \deg(f)$, and the equality holds if and only if f is totally reduced.*

Now, the polynomial mapping $\beta : \mathbb{F}_4^2 \to \mathbb{F}_4$ defined by $\beta(a_1e_1 + a_2e_2) = a_1a_2$ is totally reduced with respect to $\{e_1, e_2\}$, but

$$\beta(a_1(e_1 + e_2) + a_2e_2) = \beta(a_1e_1 + (a_1 + a_2)e_2) = a_1(a_1 + a_2) = a_1^2 + a_1a_2$$

shows that β is not totally reduced with respect to $\{e_1+e_2, e_2\}$. Hence being totally reduced is not a property of polynomial mappings. But we have:

Lemma 5.2. *Let $\alpha : V \to F$ be a polynomial mapping satisfying $\alpha(0) = 0$ and realized with respect to the basis B (respectively B^*) by the reduced polynomial f (respectively f^*). Assume that every monomial g of f satisfying $\mathrm{cdeg}(g) = \mathrm{cdeg}(f)$ is totally reduced. Then every monomial g^* of f^* satisfying $\mathrm{cdeg}(g^*) = \mathrm{cdeg}(f^*)$ is totally reduced.*

Proof. Let g be a monomial of f. Let h^* be the reduced polynomial obtained from g by the change of basis from B to B^*, and let g^* be a summand of h^*. Then $\mathrm{cdeg}(g^*) \leq \mathrm{cdeg}(h^*) = \mathrm{cdeg}(g) \leq \mathrm{cdeg}(f) = \mathrm{cdeg}(f^*)$ by Corollary 4.11, and $\deg(g^*) \leq \deg(h^*) \leq \deg(g)$. If $\mathrm{cdeg}(g^*) < \mathrm{cdeg}(f^*)$, there is nothing to prove. Assume therefore that $\mathrm{cdeg}(g^*) = \mathrm{cdeg}(f^*)$. Then $\mathrm{cdeg}(g^*) = \mathrm{cdeg}(g) = \mathrm{cdeg}(f)$, and so g is totally reduced by assumption. By Corollary 5.1, $\deg(g) = \mathrm{cdeg}(g)$. But then $\deg(g^*) \leq \deg(g) = \mathrm{cdeg}(g) = \mathrm{cdeg}(g^*)$, and the same corollary shows that $\deg(g^*) = \mathrm{cdeg}(g^*)$ and that g^* is totally reduced. □

The reader shall have no difficulty establishing:

Lemma 5.3. *Let $\alpha : V \to F$ be a polynomial mapping satisfying $\alpha(0) = 0$ and realized with respect to the basis B (respectively B^*) by the reduced polynomial f (respectively f^*). Assume that there is an integer n such that $0 \neq \deg(g) \equiv n \pmod{|F| - 1)}$ for every monomial g of f. Then $0 \neq \deg(g^*) \equiv n \pmod{|F| - 1}$ for every monomial g^* of f^*.*

Let B be a basis of V, $\alpha : V \to F$ a polynomial mapping, and f the unique reduced polynomial realizing α with respect to B. We say that $\beta : V \to F$ is a *monomial of* α if β is a polynomial mapping realized by a monomial of f.

Thanks to Lemmas 5.2 and 5.3, we can safely define the following subspaces of polynomial mappings $V \to F$ without having to fix a basis of V:

$\mathcal{P}_n(V)$=$\{\alpha;\ \mathrm{cdeg}(\alpha) \le n,\ \alpha(0) = 0\}$,
$\mathcal{P}_n^t(V)$=$\{\alpha \in \mathcal{P}_n(V);$ all monomials β with $\mathrm{cdeg}(\beta)$=n are totally reduced$\}$,
$\mathcal{P}_n^{\equiv}(V)$=$\{\alpha;$ all monomials β satisfy $0 \ne \deg(\beta) \equiv n \pmod{|F|-1}\}$.

Note that $\mathcal{P}_{n-1}(V) \subseteq \mathcal{P}_n^t(V)$.

5.2. Polynomials satisfying $\alpha(au) = a^n\alpha(u)$

Proposition 5.4. *Let $\alpha : V \to F$ be a polynomial mapping, and let $n \ge 1$. Then α satisfies* (2.3) *if and only if $\alpha \in \mathcal{P}_n^{\equiv}(V)$.*

Proof. Suppose that $\alpha \in \mathcal{P}_n^{\equiv}(V)$. Then we can make α into a not necessarily reduced homogeneous polynomial of degree $n + s(|F| - 1)$ for some s, and so $\alpha(au) = a^{n+s(|F|-1)}\alpha(u) = a^n\alpha(u)$.

Conversely, suppose that (2.3) holds. Let $B = \{e_1, \dots, e_d\}$ be a fixed basis of V, and let f be the reduced polynomial representing α with respect to B. Let M be the set of all monomials of f, $M^+ = \{g \in M;\ \deg(g) = n+s(|F|-1),\ s \ge 0\}$, and $M^- = M \setminus M^+$. If M^- is empty, we are done. Else let $\mathrm{var}(g)$ denote the set of variables present in a monomial g, and let X be a minimal element of $\{\mathrm{var}(g);\ g \in M^-\}$ with respect to inclusion. Consider a vector $v = \sum_{x_i \in X} a_ie_i$ for some $a_i \in F$. Let $g_1^+, \dots, g_r^+$ be all the monomials g of M^+ satisfying $\mathrm{var}(g) \subseteq X$, and let $g_1^-, \dots, g_s^-$ be all the monomials g of M^- satisfying $\mathrm{var}(g) \subseteq X$. Note that by the minimality of X, $\mathrm{var}(g_i^-) = X$ for every $1 \le i \le s$. Set $g^+ = g_1^+ + \dots + g_r^+$ and $g^- = g_1^- + \dots + g_s^-$. Let t_i be the degree of g_i^-. For a polynomial h, we write $h(v)$ instead of the formally correct $h(a_1, \dots, a_d)$. Then

$$\alpha(v) = g^+(v) + g^-(v),$$

and

$$\alpha(av) = a^n g^+(v) + a^{t_1}g_1^-(v) + \dots + a^{t_s}g_s^-(v).$$

On the other hand,

$$a^n\alpha(v) = a^n g^+(v) + a^n g^-(v).$$

Hence $\alpha(av) = a^n\alpha(v)$ holds if and only if

$$a^{t_1}g_1^-(v) + \dots + a^{t_s}g_s^-(v) = a^n g^-(v).$$

Note that g^- is a reduced nonzero polynomial in variables $x_i \in X$. Hence, by Lemma 2.1, there exists $v = \sum_{x_i \in X} a_i e_i$ such that $g^-(v) \neq 0$. Fix this vector v, and define a polynomial h in one variable by

$$h(x) = x^n g^-(v) - x^{t_1} g_1^-(v) - \cdots - x^{t_s} g_s^-(v).$$

This polynomial is not necessarily reduced, but since $n - t_i \not\equiv 0 \pmod{|F|-1}$ for every $1 \leq i \leq s$ and $g^-(v) \neq 0$, it does not reduce to a zero polynomial. Hence there is $a \in F$ such that $h(a) \neq 0$. But then $\alpha(av) \neq a^n \alpha(v)$ with this particular choice of a and v, a contradiction. $\square$

5.3. Polynomials with n-linear defect

Let $\alpha : V \to F$ be a polynomial mapping of combinatorial degree n. Then $\Delta^n \alpha$ is a symmetric n-additive form. Under which conditions will $\Delta^n \alpha$ be n-linear? To answer this question, we start with an example:

Example 5.5. *Let $\alpha : \mathbb{F}_4 \to \mathbb{F}_4$, $a \mapsto a^3$. Then there are two longest regular chains for the (multi)exponent* 3*, namely* $3 > 2 > 0$ *and* $3 > 1 > 0$*. Accordingly, Lemma* 4.4 *yields*

$$\Delta^2 \alpha(x, y) = \binom{3}{1} xy^2 + \binom{3}{2} x^2 y.$$

Then $\Delta^2 \alpha(x, ay) = 3xy^2a^2 + 3x^2ya$, and $a\Delta^2 \alpha(x, y) = 3xy^2a + 3x^2ya$. Hence $\Delta^2 \alpha$ is bilinear if and only if $g(x, y, a) = 3xy^2a^2 - 3xy^2a = 0$ for every $a \in \mathbb{F}_4$. Since $g(x, y, a)$ is a reduced nonzero polynomial (in variables x, y, a), it is a nonzero function by Lemma 2.1*, and thus $\Delta^2 \alpha$ is not bilinear. Why did this happen? Because not every longest regular chain for* 3 *ends in* 1*.*

To resolve the general case, first deduce from Example 4.7 and Lemmas 4.5, 4.6:

Lemma 5.6. *Let $f \in F[\overline{x}]$, $f(\overline{x}) = \overline{x}^{\overline{m}}$,* $\mathrm{char}(F) = p$*. Given a longest regular chain for $\overline{m}$, there is $j \geq 0$ such that the chain ends with a multiexponent* $(0, \ldots, 0, p^j, 0, \ldots, 0)$*. Moreover, $j = 0$ in every longest regular chain for $\overline{m}$ if and only if f is totally reduced.*

Proposition 5.7. *Let F be a field of characteristic $p \leq \infty$, and $\alpha : V \to F$ a polynomial mapping satisfying $\alpha(0) = 0$. Then $\Delta^n \alpha$ is a characteristic n-linear form if and only if $\alpha \in \mathcal{P}_n^t(V)$.*

Proof. By Lemma 3.1, every $\Delta^n\alpha$ is characteristic. To show the equivalence, it suffices to consider a monomial $\alpha(\overline{x}) = \overline{x}^{\overline{m}}$, by Lemma 4.2. If $\mathrm{cdeg}(\alpha) < n$ then $\Delta^n\alpha = 0$, and vice versa.

Assume that $\mathrm{cdeg}(\alpha) = n$. Longest regular chains for $\overline{m}$ satisfy the conclusion of Lemma 5.6. Let $a \in F$. By Lemma 4.4, any longest regular chain with $j = 0$ contributes the same monomial to $\Delta^n\alpha(a\overline{x_1}, \dots, \overline{x_n})$ and to $a\Delta^n\alpha(\overline{x_1}, \dots, \overline{x_n})$. On the other hand, every longest regular chain with $j > 0$ contributes to $\Delta^n\alpha(a\overline{x_1}, \dots, \overline{x_n})$ by a monomial containing the power a^{p^j}, while it contributes to $a\Delta^n\alpha(\overline{x_1}, \dots, \overline{x_n})$ by a monomial containing the power a^1. Hence, $\Delta^n\alpha(\overline{x_1}, \dots, a\overline{x_n}) - a\Delta^n\alpha(\overline{x_1}, \dots, \overline{x_n})$ is a reduced polynomial that is nonzero if and only if α is not totally reduced. We are then done by Lemma 2.1. □

6. The correspondence

Denote by $\mathcal{A}_n(V)$ the vector space of polynomial n-applications $V \to F$ and by $\mathcal{C}_n(V)$ the vector space of characteristic n-linear forms $V^n \to F$.

Theorem 6.1 (Correspondence). *Let V be a vector space over F. Then*

$$\mathcal{A}_n(V) = \mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V) \tag{6.1}$$

and

$$\mathcal{C}_n(V) \cong (\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V))/(\mathcal{P}_{n-1}(V) \cap \mathcal{P}_n^{\equiv}(V)). \tag{6.2}$$

Proof. The equality (6.1) follows from Propositions 5.4 and 5.7. To prove (6.2), let Ψ be the restriction of the polarization operator Δ^n to $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$. By Proposition 5.7, the image of Ψ is contained in $\mathcal{C}_n(V)$. By Theorem 3.4, Ψ is onto $\mathcal{C}_n(V)$. Clearly, the kernel of Ψ consists of $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V) \cap \mathcal{P}_{n-1}(V) = \mathcal{P}_{n-1}(V) \cap \mathcal{P}_n^{\equiv}(V)$. □

Corollary 6.2. *Let V be a d-dimensional vector space over a field F with* $\mathrm{char}(F) = \infty$. *Then $\mathcal{A}_n(V)$ are precisely the homogeneous polynomials of degree n in d variables over F, and $\mathcal{A}_n(V) \cong C_n(V)$.*

Proof. Since F is infinite, $\mathcal{P}_n^{\equiv}(V)$ consists of homogeneous polynomials of degree n. The degree and combinatorial degree of polynomials coincide over F, by Theorem 4.8. Hence $\mathcal{P}_{n-1}(V) \cap \mathcal{P}_n^{\equiv}(V)$ is trivial. As all polynomials over F are totally reduced, we have $\mathcal{P}_n^t(V) = \mathcal{P}_n(V)$ and $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V) = \mathcal{P}_n^{\equiv}(V)$. □

It is not true in general that $\mathcal{A}_n(V) = \mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$ consists only of homogeneous polynomials of degree n, as was first noticed by Prószyński in the setting of n-applications (he did not work with combinatorial degrees).

Consider the form $\alpha : \mathbb{F}_4^5 \to \mathbb{F}_4$ defined by

$$\alpha(x_1, x_2, x_3, x_4, x_5) = x_1x_2x_3x_4x_5 + x_1^2x_2^2x_3^2x_4^2. \tag{6.3}$$

Then $\mathrm{cdeg}(\alpha) = 5$ and $\deg(\alpha) = 8$. Moreover, the only monomial β of α satisfying $\mathrm{cdeg}(\beta) = 5$ is totally reduced, and the degree of every monomial of α differs from 5 by a multiple of $3 = 4 - 1$. Hence α is a 5-application. It cannot be turned into a homogeneous polynomial of degree 5 by any change of basis, by Lemma 2.2. But it can be made into a homogeneous polynomial of degree 8, for instance the polynomial

$$x_1^4x_2x_3x_4x_5 + x_1^2x_2^2x_3^2x_4^2,$$

no longer reduced.

It appears to be an interesting problem of number-theoretical flavor to characterize all pairs (V, n) for which $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$ does contain only homogeneous polynomials of degree n. It is not our intention to study this problem in detail here. Nevertheless we have the following result that shows that something interesting happens during the transition from $n = 4$ to $n = 5$ (also see Sections 2 and 3 of [6]):

Proposition 6.3. *Let $|F| = q = p^e$ and let V be a d-dimensional vector space over F. If $n < 5$ then $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$ consists of homogeneous polynomials of degree n. If $n \geq \max\{5, q\}$, $e \geq 2$, and $d \geq n$ then $\mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$ does not consist only of homogeneous polynomials of degree n.*

Proof. Let $2 \leq n < 5$, let $\alpha \in \mathcal{P}_n^t(V) \cap \mathcal{P}_n^{\equiv}(V)$, and let β be a monomial of α. We show that $\deg(\beta) \leq n$. Assume that $\deg(\beta) = n + s(q-1)$, $s > 0$. When $\mathrm{cdeg}(\beta) = n$ then β is totally reduced since $\alpha \in \mathcal{P}_n^t(V)$, and hence $\deg(\beta) = n$, a contradiction. Assume therefore that $m = \mathrm{cdeg}(\beta) < n$.

If $m = 1$, β is a scalar multiple of x^{p^i}, $i < e$, and $p^i = n + s(q-1)$. Since $s > 0$, we have $p^i > q$, a contradiction with $i < e$. If $m = 2$, β is a scalar multiple of $x^{p^i+p^j}$ or $x^{p^i}y^{p^j}$ for some $i \leq j < e$, and $p^i + p^j = n + s(q-1)$. Since $s > 0$, we have $p^i + p^j > q$, thus $p^j > q/2$, so $p^j \geq q$, a contradiction with $j < e$. If $m = 3$, we have $n = 4$, and β is a scalar multiple of $x^{p^i+p^j+p^k}$ or $x^{p^i+p^j}y^{p^k}$ or $x^{p^i}y^{p^j}z^{p^k}$. We can assume that $i \leq j \leq k < e$, and $p^i + p^j + p^k =$

$4 + s(q-1)$. Suppose that $s > 1$. Then $p^i + p^j + p^k > 2q$, thus $p^k > q/2$, a contradiction with $k < e$. Suppose that $s = 1$. Then $p^i + p^j + p^k = q + 3$. Since $p^k > q/3$, we must have $p = 2$, else $p^k \geq q$. Then $q + 3$ is odd, $p^i = 1$, $p^j + p^k > q$, $p^k > q/2$, a contradiction.

Now assume that $n \geq \max\{5, q\}$, $e \geq 2$, and $d \geq n$. Suppose for a while that there are $0 \leq a_0, \ldots, a_{e-1}$ such that

$$n + q - 1 = a_0 p^0 + \cdots + a_{e-1} p^{e-1}, \quad a_0 + \cdots + a_{e-1} < n. \tag{6.4}$$

Since $d \geq n$, we can fix a basis of V and define $\alpha : V \to F$ by setting $\alpha(x_1, \ldots, x_d)$ equal to

$$x_1 \cdots x_n + (x_1 \cdots x_{a_0})(x_{a_0+1}^p \cdots x_{a_0+a_1}^p) \cdots (x_{a_0+\cdots+a_{e-2}+1}^{p^{e-1}} \cdots x_{a_0+\cdots+a_{e-1}}^{p^{e-1}}).$$

Furthermore, α so defined satisfies $\deg(\alpha) = n + q - 1$, and

$$\mathrm{cdeg}(\alpha) = \max\{n, a_0 + \cdots + a_{e-1}\} = n.$$

The only monomial of α with combinatorial degree equal to $\mathrm{cdeg}(\alpha)$ is totally reduced, and hence α is an n-application but not a homogeneous polynomial of degree n. It remains to show that (6.4) can be satisfied.

Let $n = sp^e + r$, where $0 \leq r < p^e$ and $0 < s$. Then $n + q - 1 = sp^e + r + p^e - 1 = (sp)(p^{e-1}) + r + (p-1)(1 + p + \cdots + p^{e-1})$. Hence it is possible to write $n + q - 1 = a_0 p^0 + a_1 p^1 + \cdots + a_{e-1} p^{e-1}$ with some $0 \leq a_i$ satisfying $a_0 + \cdots + a_{e-1} \leq sp + r + (p-1)e$. A short calculation shows that $sp + r + (p-1)e \leq n$ holds if and only if $e \leq sp(1 + p + \cdots + p^{e-2})$. Since $e \geq 2$, we have $e \leq p^{e-1} \leq p(1 + p + \cdots + p^{e-2}) \leq sp(1 + p + \cdots + p^{e-2})$, and the equality holds if and only if $e = 2 = p$ and $s = 1$.

Assume that $e = 2 = p$, $s = 1$. Then $n \in \{5, 6, 7\}$, and it is easy to check in each case that (6.4) holds with a suitable choice of a_0, a_1. (For $n = 5$, we recover (6.3).) □

7. Acknowledgement

We thank the anonymous referee for several useful comments concerning the structure of this paper and for pointing out the reference [5].

References

[1] Richard A. Brualdi, Introductory Combinatorics, 4th edition, Prentice Hall, 2004.

[2] Orin Chein and Edgar G. Goodaire, *Moufang loops with a unique non-identity commutator (associator, square)*, J. Algebra **130** (1990), no. **2**, 369–384.

[3] Miguel Ferrero and Artibano Micali, *Sur les n-applications*, Colloque sur les Formes Quadratiques **2** (Montpellier, 1977), Bull. Soc. Math. France Mém. No. **59** (1979), 33–53.

[4] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.

[5] Marvin J. Greenberg, Lectures on forms in many variables, *Mathematics Lecture Note Series*, W. A. Benjamin, Inc., New York, 1969.

[6] Andrzej Prószyński, *m-applications over finite fields*, Fund. Math. **112** (1981), no. **3**, 205–214.

[7] Andrzej Prószyński, *Forms and mappings. I. Generalities*, Fund. Math. **122** (1984), no. **3**, 219–235.

[8] Andrzej Prószyński, *Forms and mappings. II. Degree* 3, Comment. Math. Prace Mat. **26** (1986), no. **2**, 309–323.

[9] Andrzej Prószyński, *Forms and mappings. III. Regular m-applications*, Comment. Math. Prace Mat. **28** (1989), no. **2**, 305–330.

[10] Andrzej Prószyński, *Forms and mappings. IV. Degree* 4, Bull. Polish Acad. Sci. Math. **37** (1989), no. **1-6**, 269–278.

[11] Thomas M. Richardson, *Local subgroups of the Monster and odd code loops*, Trans. Amer. Math. Soc. **347** (1995), no. **5**, 1453–1531.

[12] Petr Vojtěchovský, *Combinatorial polarization, code loops, and codes of high level*, proceedings of CombinaTexas 2003, published in the International Journal of Mathematics and Mathematical Sciences **29** (2004), 1533–1541.

[13] Harold N. Ward, *Combinatorial polarization*, Discrete Math. **26** (1979), no. **2**, 185–197.