FORMS OF ALL DEGREES

ALEŠ DRÁPAL AND PETR VOJTĚCHOVSKÝ

Abstract. Let F be a field and V a finite-dimensional vector space over F. Given $\alpha : V \to F$ and $n \geq 1$, let $\alpha_n(u_1, \dots, u_n) = \sum(-1)^{n-m}\alpha(u_{i_1} + \cdots + u_{i_m})$, where the summation ranges over all subsets $\{i_1, \dots, i_m\}$ of $\{1, \dots, n\}$. This process is called combinatorial polarization. The combinatorial degree of α is the unique integer n such that $\alpha_n \neq 0$ and $\alpha_{n+1} = 0$.

A map $\alpha : V \to F$ is a *form of degree* n if α_n is a symmetric n-linear form and $\alpha(au) = a^n\alpha(u)$ for every $a \in F$, $u \in V$. Forms of degree 2 are precisely quadratic forms. A symmetric form $\varphi : V^n \to F$ is said to be *characteristic* if it vanishes whenever one of its arguments is repeated at least $\mathrm{char}(F)$ times.

We investigate the relationship between forms of degree n, characteristic n-linear forms, and homogeneous polynomials of degree n. In particular: (i) we show how to compute the combinatorial degree of any polynomial map, (ii) we prove that a symmetric n-linear form φ can be obtained from some map $\alpha : V \to F$ by combinatorial polarization if and only if φ is characteristic, and in such a case α can be chosen uniquely as a homogeneous polynomial of degree n with all exponents less than $\mathrm{char}(F)$, (iii) given a characteristic n-linear form φ, we describe all polynomial forms α of degree n such that $\alpha_n = \varphi$, (iv) we describe all polynomials satisfying the condition $\alpha(au) = a^n\alpha(u)$, and all polynomials α for which α_n is symmetric n-linear, (v) we show that for $n \geq 5$ there are forms of degree n that cannot be viewed as homogeneous polynomials of degree n, but only as homogeneous polynomials of degree $n + s(|F| - 1)$ for some $s > 0$. In doing so, we recover many classical results for quadratic forms as a special case.

The question whether every form of degree $n > 2$ must be a polynomial map is answered affirmatively in many situations, but the general case remains open.

1. Introduction

Two is the oddest prime. Every student of abstract algebra learns early on to treat calculations over fields of characteristic two with special care, and becomes used to the experience that a proof that works in all odd characteristics has to be modified in characteristic two, if it can be salvaged at all. The purpose of this paper is to show that this dichotomy is out of place in at least one well-known instance, namely while dealing with the quadratic forms.

We do not claim that quadratic forms do not behave differently in characteristic two—they do. Instead, we generalize the concept of a quadratic form to obtain *forms of degree* $n \geq 2$, using combinatorial polarization, and show that the phenomena encountered with quadratic forms in characteristic two are analogously encountered for all forms of degree n in all characteristics $p \leq n$. We pay special attention to the relationship between forms of degree n, a class of symmetric n-linear forms called *characteristic* here, and homogenous polynomials. The aforementioned homogeneous polynomials have degree n when $n < 5$,

2000 *Mathematics Subject Classification.* Primary: 11E76. Secondary: 11E04, 11C08, 05E05.

Key words and phrases. quadratic form, cubic form, form of degree n, n-additive form, n-linear form, symmetric n-linear form, characteristic form, combinatorial polarization, combinatorial degree, homogeneous polynomial, polynomial map.

The final version of this paper was written while the first author was visiting University of Wisconsin-Madison as a Fulbright research scholar. He was also supported by institutional grant MSM 0021620839 and by Grant Agency of Charles University, grant 444/2004.

but when $n \geq 5$, their degrees can be higher by a multiple of $|F| - 1$, where F is the underlying field.

This paper was not written to mindlessly generalize the concept of a quadratic form. Rather, it has developed from our need to understand why the prime three behaves differently from all other primes for Richardson's odd code loops [4]. The reason turned out to be the fact that odd code loops are connected to characteristic trilinear forms, and hence to forms of degree three. The details of this connection to code loops, and thus indirectly to the Monster group, will be presented separately in a later paper.

In Sections 2–6 we deal with the necessary prerequisites concerning polynomial maps, combinatorial degree, and quadratic forms. Forms of degree n are defined in Section 7. The main results are formulated in Sections 9–11. We were not able to answer all questions that arise naturally from our investigation; see Section 12.

2. Basic terminology and notation

Throughout the paper, p is a prime, F is a field, V is a d-dimensional vector space over F, $q = p^e$ for some $e > 0$, and $\mathbb{F}_q$ is the q-element field. The characteristic of F is denoted by $\mathrm{char}(F)$. We find it convenient to follow the classical literature and set $\mathrm{char}(F) = \infty$ for all fields F containing the rational numbers, instead of the more contemporary $\mathrm{char}(F) = 0$.

2.1. **Forms.** 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, $\dots$, $v_n \in V$. Note that a symmetric n-additive form is automatically n-linear when F is a prime field.

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, $f(r * u, s * v)$ stands for

$$f(\underbrace{u, \dots, u}_{r \text{ times}}, \underbrace{v, \dots, v}_{s \text{ times}}).$$

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

The vector space of symmetric n-linear forms $V^n \to F$ will be denoted by $\mathrm{LinF}(V, n)$, and the vector space of characteristic forms $V^n \to F$ by $\mathrm{CharF}(V, n)$.

2.2. **Combinatorial polarization.** Symmetric multiadditive forms can be built from maps $V \to F$ by a process called *combinatorial polarization*, devised by Ward [6].

Let $\alpha : V \to F$ be a form satisfying $\alpha(0) = 0$, and let $n \geq 1$. The *nth derived form* $\alpha_n : V^n \to F$ *of* α is defined by

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

Then α_n 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

$$\begin{aligned} \alpha_n(u, v, w_3, \dots, w_n) = {} & \alpha_{n-1}(u + v, w_3, \dots, w_n) \\ & - \alpha_{n-1}(u, w_3, \dots, w_n) - \alpha_{n-1}(v, w_3, \dots, w_n). \end{aligned} \tag{2.2}$$

If there is a positive integer n such that $\alpha_n \neq 0$ and $\alpha_{n+1} = 0$, we say that α has *combinatorial degree* n, and we write $\mathrm{cdeg}(\alpha) = n$. If α is the zero map, we set $\mathrm{cdeg}(\alpha) = -1$. Note that $\mathrm{cdeg}(\alpha)$ is not defined for every α, but such maps will not concern us here.

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

Combinatorial polarization is a linear process, i.e., $(c\alpha + d\beta)_n = c\alpha_n + d\beta_n$ for every c, $d \in F$ and α, $\beta : V \to F$.

2.3. **Multivariate polynomials.** Let $F[x_1, \dots, x_d]$ be the ring of polynomials in variables $x_1, \dots, x_d$ 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 multiexponents of f.

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

3. Multivariate polynomials and polynomial maps

Allow us to collect elementary results on multivariate polynomials and polynomial maps in this section.

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 $|F| - 1$. 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 a congruence 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.

A polynomial $f \in F[\overline{x}]$ is the *zero function* if $f(a_1, \dots, a_d) = 0$ for every $a_1, \dots, a_d \in F$.

Lemma 3.1. *Let f, $g \in F[\overline{x}]$. Then $[f]_\sim = [g]_\sim$ if and only if $f - g$ is the zero function.*

Proof. Assume that $[f]_\sim = [g]_\sim$. Then for every $\overline{m} \in M(f)$ there is $\overline{n} \in M(g)$ such that $c(\overline{m}) = c(\overline{n})$ and $m_i \equiv n_i \pmod{|F| - 1}$ for every $1 \leq i \leq d$. Thus $a^{m_i} = a^{n_i}(a^{(|F|-1)})^k = a^{n_i}$ for some k, and so $f(a_1, \dots, a_d) = g(a_1, \dots, a_d)$ follows.

To show the converse, assume that f, g are reduced and $h = f - g$ is the zero function.

Suppose that $d = 1$. Then h is a univariate polynomial and every element of F is a root of h. This is clearly impossible when F is infinite. When F is finite then $\deg(h) \leq |F| - 1$ because h is reduced, again a contradiction.

Assume that $d > 1$ and that the implication holds for every reduced nonzero polynomial in at most $d - 1$ variables. Write h as

$$h(x_1, \dots, x_d) = \sum_i h_i(x_1, \dots, x_{d-1})x_d^i,$$

for some $h_i \in F[x_1, \dots, x_{d-1}]$. If $h_i = 0$ for every $i > 0$ we are done by the induction hypothesis. So assume that $h_j \neq 0$ for some $j > 0$. Since h_j is reduced, there are $a_1, \dots, a_{d-1} \in F$ such that $h_j(a_1, \dots, a_{d-1}) \neq 0$, by the induction hypothesis. Then $h(a_1, \dots, a_{d-1}, x_d) \in F[x_d]$ is a nonzero reduced polynomial in one variable, and there is some $a_d \in F$ such that $h(a_1, \dots, a_d) \neq 0$. $\square$

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

$$\alpha\left(\sum_{i=1}^{d} a_i e_i\right) = f(a_1, \dots, a_d)$$

for every $a_1, \dots, a_d \in F$. We say that f *realizes* α *with respect to* B. By Lemma 3.1, there is a unique reduced polynomial realizing α with respect to B.

Proposition 3.2. *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^*. Moreover:*

(i) $\deg(f) = \deg(f^*)$,

(ii) *if f has the property that* $\deg(g) \equiv n \pmod{|F| - 1}$ *for all monomials g of f and some fixed n, then f^* has the same property.*

Proof. Let $B = \{e_1, \dots, e_d\}$, $B^* = \{e_1^*, \dots, e_d^*\}$, $e_i^* = \sum_j b_{ij} e_j$. Then

$$\alpha\big(\sum_i a_i e_i^*\big) = \alpha\big(\sum_i a_i \sum_j b_{ij} e_j\big) = \alpha\big(\sum_j \big(\sum_i a_i b_{ij}\big) e_j\big) = f\big(\sum_i a_i b_{i1}, \dots, \sum_i a_i b_{id}\big). \tag{3.1}$$

It is now obvious that the right hand side is a polynomial in $a_1, \dots, a_d$.

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

$$g\big(\sum_i x_i b_{i1}, \dots, \sum_i x_i b_{id}\big) = \big(\sum_i x_i b_{i1}\big)^{m_1} \cdots \big(\sum_i x_i b_{id}\big)^{m_d}, \tag{3.2}$$

and the multinomial theorem implies that every summand on the right hand side of (3.2) has degree $m_1 + \cdots + m_d$. Upon reducing the right hand side, the exponents can either decrease by a multiple of $|F| - 1$, or remain the same. This shows (ii).

The change of basis $(b_{ij})_{i,j=1}^d$ can be decomposed as a product of the two elementary row operations: (a) multiplying row i by a nonzero constant c, (b) replacing row i with the sum of rows $i \neq j$. It therefore suffices to prove (i) for (a) and (b). With respect to these row operations with $i = 1$, $j = 2$, the right hand side of (3.2) becomes

$$(cx_1)^{m_1} x_2^{m_2} \cdots x_d^{m_d}, \quad (x_1 + x_2)^{m_1} x_2^{m_2} \cdots x_d^{m_d},$$

respectively. Since no reduction is needed for (a), we focus on (b). Let $M^+ = \{\overline{m} \in M(f);\ m_1 + \cdots + m_d = \deg(f)\}$, and let $\overline{m}$ be a maximal element of M^+ with respect to the lexicographic order. Let $g(\overline{x}) = \overline{x}^{\overline{m}}$. Upon applying (b) to g, it becomes $(x_1 + x_2)^{m_1} x_2^{m_2} \cdots x_d^{m_d}$, and it contains the reduced summand $x_1^{m_1} \cdots x_d^{m_d}$. We now show that this summand will not vanish by cancelation upon applying (b) to f. Should this happen, there would be another $\overline{n} \in M(f)$ such that

$$(x_1 + x_2)^{n_1} x_2^{n_2} \cdots x_d^{n_d} = \sum_{k=0}^{n_1} \binom{n_1}{k} x_1^k x_2^{n_1 - k + n_2} x_3^{n_3} \cdots x_d^{n_d}$$

contains $x_1^{m_1} \cdots x_d^{m_d}$. Thus $n_i = m_i$ for $i > 2$, and there is $0 \le k \le n_1$ such that $k = m_1$ and $n_1 - k + n_2 = m_2$. By the maximality of $\overline{m}$, we have $m_1 = k \le n_1 \le m_1$. Thus $n_1 = m_1$, $n_2 = m_2$, and $\overline{n} = \overline{m}$. □

A map $\alpha : V \to F$ is a *polynomial map of degree* n if α is realized by a reduced polynomial of degree n with respect to some basis B of V.

We have just shown that this concept is well-defined, and that for every choice of a basis for V there is an isomorphism between the vector space of polynomial maps $V \to F$ of degree at most n, and the vector space of reduced polynomials of degree at most n in d variables over F.

Every map $\alpha : V \to F$ is a polynomial map when F is finite:

Theorem 3.3 (Lagrange interpolation over $\mathbb{F}_q$)**.** *Let V be a vector space over $\mathbb{F}_q$ with basis $\{e_1, \dots, e_d\}$. Then for every map $\alpha : V \to \mathbb{F}_q$ there exists a unique reduced polynomial $f \in \mathbb{F}_q[\overline{x}]$ such that $\alpha(\sum a_i e_i) = f(a_1, \dots, a_d)$ for every $a_1, \dots, a_d \in \mathbb{F}_q$.*

Proof. It remains to establish the existence. In the degenerate case $d = 0$, let f be the constant $\alpha(0)$. Else assume that $d > 0$ and that the lemma holds in dimension less than d. For $a \in \mathbb{F}_q$, let $\alpha[a] : \langle e_2, \dots, e_d\rangle \to \mathbb{F}_q$ be defined by

$$\alpha[a](a_2e_2 + \cdots + a_de_d) = \alpha(ae_1 + a_2e_2 + \cdots + a_de_d),$$

and let $f[a]$ be the polynomial obtained by the lemma for the map $\alpha[a]$. Then

$$f(x_1, \dots, x_d) = \sum_{a\in\mathbb{F}_q} f[a](x_2, \dots, x_d) \prod_{b\neq a} \frac{x_1 - b}{a - b}$$

does the job, upon reducing it if necessary. □

4. Combinatorial degree of polynomials

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-ary digits of* t, satisfying $0 \le t_i < p$ 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 [6], 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 map satisfying $\alpha(0) = 0$. Then* $\mathrm{cdeg}(\alpha) = \deg(\alpha)$*.*

He also mentioned [6, 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 in [5].

In this section, we generalize the above results and give a proof for polynomials over any field. We follow [5] very closely, and start by developing combinatorial polarization for formal polynomials.

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 $f \in F[\overline{x}]$ and $n \ge 1$, let $f_n \in F[x_{1,1}, \dots, x_{1,d}, \dots, x_{n,1}, \dots, x_{n,d}]$ be defined by

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

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

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

Lemma 4.2. *If f, $g \in F[\overline{x}]$ satisfy $M(f) \cap M(g) = \emptyset$ then $M(f_n) \cap M(g_n) = \emptyset$ 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 $f_n(\overline{x_1}, \dots, \overline{x_n})$, 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 $1 \leq i \leq d$, the variables $x_{1,i}, \dots, x_{s,i}$ appear in h precisely m_i times, counting multiplicities. Hence the multiexponent $\overline{m}$ can be reconstructed from any monomial of $f_n(\overline{x_1}, \dots, \overline{x_n})$. □

Corollary 4.3. *Let $f \in F[\overline{x}]$. Then* $\mathrm{cdeg}(f) = \max\{\mathrm{cdeg}(\overline{x}^{\overline{m}});\ \overline{m} \in M(f)\}$.

We proceed to determine the combinatorial degree of monomials.

Let $\overline{m}$, $\overline{n}$ be two multiexponents. We write $\overline{m} \leq \overline{n}$ if $m_i \leq n_i$ for every $1 \leq i \leq d$. When $\overline{m} \leq \overline{n}$, $\overline{n} - \overline{m}$ stands for the multiexponent $(n_1 - m_1, \dots, n_d - m_d)$. 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 derived forms of monomials.

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

$$f_s(\overline{x_1}, \dots, \overline{x_s}) = \sum \binom{\overline{m_1}}{\overline{m_2}} \cdots \binom{\overline{m_{s-1}}}{\overline{m_s}} \overline{x_1}^{\overline{m_s}} \overline{x_2}^{\overline{m_{s-1}} - \overline{m_s}} \cdots \overline{x_s}^{\overline{m_1} - \overline{m_2}}, \tag{4.2}$$

where the summation runs 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

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

Since $f_2(\overline{x}, \overline{y}) = (\overline{x} + \overline{y})^{\overline{m}} - \overline{x}^{\overline{m}} - \overline{y}^{\overline{m}}$, the lemma follows for $s = 2$.

Let $g(\overline{x}) = \overline{x}^{\overline{m_s}}$. We have just shown that

$$g_2(\overline{x_1}, \overline{x_2}) = \sum_{0 < \overline{m_{s+1}} < \overline{m_s}} \binom{\overline{m_s}}{\overline{m_{s+1}}} \overline{x_1}^{\overline{m_{s+1}}} \overline{x_2}^{\overline{m_s} - \overline{m_{s+1}}}. \tag{4.3}$$

Assume that the lemma holds for s. Using the recurrence relation (2.2), we obtain

$$f_{s+1}(\overline{x_1}, \dots, \overline{x_{s+1}}) = \sum \binom{\overline{m_1}}{\overline{m_2}} \cdots \binom{\overline{m_{s-1}}}{\overline{m_s}} g_2(\overline{x_1}, \overline{x_2}) \overline{x_3}^{\overline{m_{s-1}} - \overline{m_s}} \cdots \overline{x_{s+1}}^{\overline{m_1} - \overline{m_2}}.$$

Substituting (4.3) into the last equation yields the result. □

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 the 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 $1 \le i < s$, 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 $0 \le n_i < p$ 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 $0 \le a_i,\ b_i < p$ for every i. By Lucas Theorem [3],

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

modulo p. Consequently, if $\binom{a}{b} \not\equiv 0$, we must have $a_i \ge b_i$ 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, $t \ge \omega_p(n)$ 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. □

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 $1 \le i < s$, and $s = \sum_{i=1}^{d} \omega_p(m_i)$, where $p = \mathrm{char}(F) \le \infty$.*

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. □

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 have:

Theorem 4.8 (Combinatorial degree of formal polynomials)**.** *Let $f \in F[\overline{x}]$, $\mathrm{char}(F) = p \le \infty$. Then $\mathrm{cdeg}(f) = \deg_p(f)$.*

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

Lemma 4.9. *Let $f \in F[\overline{x}]$ be a reduced polynomial. Then $f_n \in F[\overline{x_1}, \ldots, \overline{x_n}]$ is a reduced polynomial for every $n \ge 1$.*

Lemma 4.10. *Let $\alpha : V \to F$ be a polynomial map, 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 $n \ge 1$, and $u_i = \sum_j a_{ij} e_j$. Then

$$\alpha_n(u_1, \ldots, u_n) = \alpha\Big(\sum_j a_{1j} e_1, \ldots, \sum_j a_{nj} e_j\Big) = f_n(a_{11}, \ldots, a_{1d}, \ldots, a_{n1}, \ldots, a_{nd}). \tag{4.5}$$

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

On the other hand, assume that $n = \mathrm{cdeg}(f)$. Then f_n is a nonzero polynomial that is reduced by Lemma 4.9. Thus f_n is a nonzero function by Lemma 3.1, and (4.5) implies that $\mathrm{cdeg}(\alpha) \geq n = \mathrm{cdeg}(f)$. $\square$

Corollary 4.11 (Combinatorial degree of polynomial maps)**.** *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 map satisfying $\alpha(0) = 0$. Then $\mathrm{cdeg}(\alpha)$ is equal to $\deg_p(f)$, where $f \in F[x_1, \dots, x_d]$ is the reduced polynomial that realizes α with respect to a basis of V.*

5. Homogeneous and totally reduced polynomials

We have already established that the degree of a polynomial map is well-defined. By Corollary 4.11, the combinatorial degree is also well-defined for polynomial maps.

However, one has to be careful with even the most common concepts, such as the property of being homogeneous (i.e., all monomials having the same degree). To see this, consider the polynomial map $\alpha : \mathbb{F}_4^2 \to \mathbb{F}_4$ defined by $\alpha(a_1e_1 + a_2e_2) = a_1^2a_2^2$ with respect to some basis $\{e_1, e_2\}$. Then

$$\alpha(a_1(e_1 + e_2) + a_2e_2) = \alpha(a_1e_1 + (a_1 + a_2)e_2) = a_1^2(a_1 + a_2)^2 = a_1^4 + a_1^2a_2^2 = a_1 + a_1^2a_2^2.$$

Thus α is homogeneous with respect to $\{e_1, e_2\}$ but not with respect to $\{e_1 + e_2, e_2\}$, as a reduced polynomial.

If we do not insist on polynomials being reduced, then the situation can be remedied: A change of basis applied to a reduced homogeneous polynomial of degree n will produce a reduced polynomial of degree n in which the degrees of any two monomials differ by a multiple of $|F| - 1$, by Proposition 3.2. Hence the resulting reduced polynomial can be turned into a homogeneous polynomial of degree n, albeit not necessarily reduced.

No such "trick" works for the following property of polynomials: A polynomial $f \in F[x_1, \dots, x_d]$ 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 map $\beta : \mathbb{F}_4^2 \to \mathbb{F}_4$ 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 $\{e_1 + e_2, e_2\}$.

Nevertheless we have:

Lemma 5.2. *Let $\alpha : V \to F$ be a polynomial map 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 f^* has the same property.*

Proof. Let g be a monomial of f. Let g^* be the reduced polynomial obtained from g by the change of basis from B to B^*, and let h^* be a summand of g^*. Then $\mathrm{cdeg}(h^*) \leq \mathrm{cdeg}(g^*) = \mathrm{cdeg}(g) \leq \mathrm{cdeg}(f) = \mathrm{cdeg}(f^*)$ by Theorem 4.8, and $\deg(h^*) \leq \deg(g^*) \leq \deg(g)$. If $\mathrm{cdeg}(h^*) < \mathrm{cdeg}(f^*)$, we do not care whether h^* is totally reduced or not. Assume that $\mathrm{cdeg}(h^*) = \mathrm{cdeg}(f^*)$. Then $\mathrm{cdeg}(h^*) = \mathrm{cdeg}(g) = \mathrm{cdeg}(f)$, so g is totally reduced by assumption. By Corollary 5.1, $\deg(g) = \mathrm{cdeg}(g)$. But then $\deg(h^*) \leq \deg(g) = \mathrm{cdeg}(g) = \mathrm{cdeg}(h^*)$, and the same corollary shows that $\deg(h^*) = \mathrm{cdeg}(h^*)$ and h^* is totally reduced. $\square$

We can now safely define the following subspaces of polynomial maps $V \to F$:

$$\begin{aligned}
\mathrm{Pol}(V,n) =&\{\alpha;\ \mathrm{cdeg}(\alpha)\le n\},\\
\mathrm{Pol}_{tot}(V,n) =&\{\alpha\in\mathrm{Pol}(V,n);\ \text{all monomials } \beta \text{ of } \alpha \text{ with } \mathrm{cdeg}(\beta)=n \text{ are totally reduced}\},\\
\mathrm{Pol}_{\equiv}(V,n) =&\{\alpha;\ \text{all monomials } \beta \text{ of } \alpha \text{ satisfy } 0\ne\deg(\beta)\equiv n \pmod{|F|-1}\}.
\end{aligned}$$

When F is infinite, the condition $\deg(\beta)\equiv n \pmod{|F|-1}$ says merely that α is homogeneous of degree n.

6. Quadratic forms versus quadratic homogeneous polynomials

Let us recall some well-known facts about quadratic forms that will motivate the more general results discussed below. All facts stated without proof in this section will be established more generally later.

A *quadratic form* $\alpha : V \to F$ is a map satisfying

$$\alpha(au) = a^2\alpha(u) \tag{6.1}$$

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

$$\varphi(u,v) = \alpha(u+v) - \alpha(u) - \alpha(v) \tag{6.2}$$

is a symmetric bilinear form. We say that φ is *associated* with α. Note that φ is equal to α_2, the second derived form of α.

Quadratic forms are often defined as homogeneous quadratic polynomials $V \to F$. Apart from the small hiccup while dealing with a change of basis (see Section 5), the two definitions are equivalent.

Let us clarify this point by considering the following question: *Given a symmetric bilinear form $\varphi : V \times V \to F$, what are all the quadratic forms with which φ is associated, if any?*

Assume that $\mathrm{char}(F) \ne 2$. Then

$$\varphi(u,u) = \alpha(2u) - 2\alpha(u) = 2\alpha(u),$$

so there is precisely one quadratic form with which φ is associated, namely

$$\alpha(u) = \frac{\varphi(u,u)}{2}. \tag{6.3}$$

With respect to a fixed basis $\{e_1,\dots,e_d\}$ of V, equation (6.3) becomes

$$\alpha\Big(\sum_i a_ie_i\Big) = \frac{1}{2}\Big(\sum_i a_i^2\varphi(e_i,e_i) + 2\sum_{i<j} a_ia_j\varphi(e_i,e_j)\Big), \tag{6.4}$$

and thus α can be regarded as a homogeneous quadratic polynomial. Note that α is totally reduced.

Suppose that $\mathrm{char}(F) = 2$ and $\varphi(u,u) \ne 0$ for some $u \in V$. Then φ is associated with no quadratic form, as $\alpha(2u) - 2\alpha(u) = 0$.

Suppose that $\mathrm{char}(F) = 2$ and $\varphi(u,u) = 0$ for every $u \in V$ (i.e., φ is characteristic). Then one can show that φ is associated with the totally reduced homogeneous quadratic polynomial

$$\alpha(\sum a_ie_i) = \sum_{i<j} a_ia_j\varphi(e_i,e_j), \tag{6.5}$$

since the first sum of (6.4) vanishes, and we can "cancel" the twos in (6.4). But (6.5) is not the only quadratic from with which φ is associated. We can add any quadratic homogeneous polynomial of combinatorial degree less than two to (6.5), as this will have no effect on $\alpha_2 = \varphi$, and the property $\alpha(au) = a^2\alpha(u)$ will still hold. Thus every quadratic form

$$\sum_{i<j} a_i a_j \varphi(e_i, e_j) + \sum_i c_i a_i^2 \tag{6.6}$$

yields φ, and it is not difficult to see that φ is associated with no other polynomials. In fact, only polynomial maps can be associated with φ:

Lemma 6.1. *Every quadratic form is a polynomial map.*

Proof. Let β be a quadratic from with associated symmetric bilinear form φ. Then φ is also associated with a quadratic homogeneous polynomial α given by (6.4) or (6.5). For $\gamma = \beta - \alpha$, we have

$$\gamma(u+v) = \beta(u+v)+\alpha(u+v) = \beta(u)+\beta(v)+\varphi(u,v)-\alpha(u)-\alpha(v)-\varphi(u,v) = \gamma(u)+\gamma(v).$$

With respect to a basis $\{e_1, \dots, e_d\}$ of V we therefore have $\gamma(\sum a_i e_i) = \sum \gamma(a_i e_i) = \sum a_i^2 \gamma(e_i)$, which shows that both γ and $\beta = \alpha + \gamma$ are polynomial maps. □

Therefore, quadratic forms are indeed precisely homogeneous quadratic polynomials in any characteristic. This, however, *is a coincidence.*

7. Defining forms of degree n

Generalizing (6.1) and (6.2) in a straightforward way, we arrive at the concept of a form of degree n:

Let V be a vector space over F, and $\alpha : V \to F$ a map. Then α is a *form of degree n* if

$$\alpha(au) = a^n \alpha(u) \tag{7.1}$$

for every $a \in F$, $u \in V$, and if $\varphi : V^n \to F$ defined by

$$\varphi = \alpha_n \tag{7.2}$$

is a symmetric n-linear form. We say that φ is *associated* with α.

Our goal is to understand the relationship between forms of degree n, characteristic n-linear forms, and homogeneous polynomials.

Unlike in the case $n = 2$, we do not know if a form of degree $n > 2$ has to be a polynomial map. We will revisit this question at the end of the paper. Meanwhile, we will fully describe the case of forms of degree n that are polynomial maps.

8. The condition $\alpha(au) = a^n\alpha(u)$

In this section we characterize all polynomial maps $\alpha : V \to F$ satisfying the condition (7.1).

Proposition 8.1. *Let $\alpha : V \to F$ be a polynomial map, and let $n \geq 1$. Then α satisfies* (7.1) *if and only if $\alpha \in \mathrm{Pol}_\equiv(V, n)$.*

Proof. Suppose that $\alpha \in \mathrm{Pol}_\equiv(V, n)$. Then we can make α into a 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 (7.1) 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, $M^+ = \{g \in M;\ \deg(g) = n+s(|F|-1),\ s \in \mathbb{Z}\}$, 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 $v = \sum_{x_i \in X} a_i e_i$ 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 $g^+ = g_1^+ + \cdots + g_r^+$ and $g^- = g_1^- + \cdots + g_s^-$. Let t_i be the degree of g_i^-. For a polynomial h, we write $h(v)$ instead of the formally correct $h(a_1, \ldots, a_d)$. Then

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

and

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

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

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

Note that g^- is a reduced nonzero polynomial in variables $x_i \in X$. Hence, by Lemma 3.1, 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 $1 \le i \le s$ 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. □

9. When does combinatorial polarization yield n-linear forms?

Let $\alpha : V \to F$ be a polynomial map of combinatorial degree n. Then α_n is a symmetric n-additive form. This form is automatically n-linear over prime fields, but not necessarily over all fields. What are the conditions on α so that α_n is n-linear? To answer this question, we start with an example:

Let $\alpha : \mathbb{F}_4 \to \mathbb{F}_4$, $a \mapsto a^3$. Then there are 2 longest regular chains for the (multi)exponent 3, namely $3 > 2 > 0$ and $3 > 1 > 0$. (See Section 4.) Accordingly, Lemma 4.4 yields $\alpha_2(x, y) = \binom{3}{1} xy^2 + \binom{3}{2} x^2 y$. Then $\alpha_2(x, ay) = 3xy^2a^2 + 3x^2ya$, and $a\alpha_2(x, y) = 3xy^2a + 3x^2ya$. Hence α_2 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 3.1, and thus α_2 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 9.1. *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 $j \ge 0$ 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 9.2. *Let F be a field of characteristic $p \le \infty$, and $\alpha : V \to F$ a polynomial map. Then α_n is a symmetric n-linear form if and only if $\alpha \in \mathrm{Pol}_{tot}(V, n)$.*

Proof. By Lemma 4.2 it suffices to prove the theorem for all monomials $\alpha(\overline{x}) = \overline{x}^{\overline{m}}$. If $\mathrm{cdeg}(\alpha) < n$ then $\alpha_n = 0$ is certainly a symmetric n-linear form.

Assume that $\mathrm{cdeg}(\alpha) = n$. Longest regular chains for $\overline{m}$ satisfy the conclusion of Lemma 9.1. Let $a \in F$. By Lemma 4.4, any longest regular chain with $j = 0$ contributes the same monomial to $\alpha_n(a\overline{x_1}, \ldots, \overline{x_n})$ and to $a \cdot \alpha_n(\overline{x_1}, \ldots, \overline{x_n})$. On the other hand, every longest regular chain with $j > 0$ contributes to $\alpha_n(a\overline{x_1}, \ldots, \overline{x_n})$ by a monomial containing the power a^{p^j}, while it contributes to $a \cdot \alpha_n(\overline{x_1}, \ldots, \overline{x_n})$ by a monomial containing the power a^1. Hence, $\alpha_n(\overline{x_1}, \ldots, a\overline{x_n}) - a \cdot \alpha_n(\overline{x_1}, \ldots, \overline{x_n})$ is a reduced polynomial that is nonzero if and only if α is not totally reduced. We are then done by Lemma 3.1. □

Theorem 9.3 (Polynomial forms of degree n)**.** *For every $n \geq 1$ we have*

$$\{\alpha : V \to F;\ \alpha \text{ is a polynomial form of degree } n\} \cong \mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$$

as vector spaces.

Proof. Let α be a polynomial map that is a form of degree n. By Proposition 9.2, $\alpha \in \mathrm{Pol}_{tot}(V,n)$. By Proposition 8.1, $\alpha \in \mathrm{Pol}_{\equiv}(V,n)$. The converse holds since the two propositions are equivalences. □

Corollary 9.4. *Let $n \geq 1$, and let V be a vector space over a field F of characteristic ∞. Then the vector space of polynomial forms $\alpha : V \to F$ of degree n is isomorphic to the vector space of homogeneous polynomials of degree n.*

However, it is not true in general that $\mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$ consists only of homogeneous polynomials of degree n.

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

$$\alpha(x_1,x_2,x_3,x_4,x_5) = x_1x_2x_3x_4x_5 + x_1^2x_2^2x_3^2x_4^2. \tag{9.1}$$

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 form of degree 5. It cannot be turned into a homogeneous polynomial of degree 5 by any change of basis, by Proposition 3.2. But it can be made into a homogeneous polynomial of degree 8; for instance the polynomial

$$\alpha^*(x_1,x_2,x_3,x_4,x_5) = x_1^2x_2^2x_3^2x_4^2 + x_1^4x_2x_3x_4x_5,$$

no longer reduced.

It appears to be an interesting problem of number-theoretical flavor to characterize all pairs (V,n) for which $\mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$ 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 $n = 5$:

Proposition 9.5. *Let $|F| = q = p^e$ and let V be a d-dimensional vector space over F. If $n < 5$ then $\mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$ consists of homogeneous polynomials of degree n. If $n \geq \max\{5,q\}$, $e \geq 2$, and $d \geq n$ then $\mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$ does not consist only of homogeneous polynomials of degree n.*

Proof. Let $2 \leq n < 5$, let $\alpha \in \mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}_{\equiv}(V,n)$, 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, and hence $\deg(\beta) = n$. Assume 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 scalar multiple of $x^{p^i+p^j+p^k}$ or $x^{p^i+p^j}y^{p^k}$ or $x^{p^i}y^{p^j}z^{p^k}$. Upon relabelling, we can assume that $i \leq j \leq k < e$, and $p^i + p^j + p^k = 4 + s(q-1)$. Assume that $s > 1$. Then $p^i + p^j + p^k > 2q$, thus $p^k > q/2$, a contradiction with $k < e$. Assume that $s = 1$. Then $p^i + p^j + p^k = q + 3$. Since $p^k > q/3$, we must have $p = 2$. If $p^j < q/2$ then $p^i + p^j + p^k \leq q/4 + q/4 + q/2$, a contradiction. Thus $p^j = p^k = q/2$. Then $p^i = 3$, a contradiction.

Now assume that $n \geq \max\{5,q\}$, $e \geq 2$, and $d \geq n$. 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 $n + q - 1$ as a sum $a_0p^0 + a_1p^1 + \cdots + a_{e-1}p^{e-1}$ with some $a_i \geq 0$ satisfying $a_0 + \cdots + a_{e-1} \leq sp + r + (p-1)e$.

If

$$sp + r + (p-1)e \leq n, \tag{9.2}$$

we can fix a basis of V and define $\alpha : V \to F$ by

$$\alpha(x_1, \dots, x_d) = x_1 \cdots x_n + (x_1 \cdots x_{a_0})(x_{a_0+1}^p \cdots x_{a_0+a_1}^p) \cdots (x_{a_0+\cdots+a_{e-2}+1}^{p^{e-1}} \cdots x_{a_0+\cdots+a_{e-1}}^{p^{e-1}}),$$

because $n \leq d$. Furthermore, α so defined satisfies $\deg(\alpha) = n + q - 1$, and $\mathrm{cdeg}(\alpha) = \max\{n, a_0 + \cdots + a_{e-1}\} = n$. If the inequality of (9.2) is strict, the only summand of α with combinatorial degree equal to $\mathrm{cdeg}(\alpha)$ is totally reduced, hence α is a form of degree n, but not a homogeneous polynomial of degree n.

A short calculation shows that (9.2) 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 only if and only if $e = p = 2$ and $s = 1$. Assume that $e = p = 2$ and $s = 1$. Then $n \in \{5, 6, 7\}$, and it suffices to show that $n + q - 1$ can be written as $a_0 + 2a_1$ for some a_0, a_1 with $a_0 + a_1 < n$. When $n = 5$, we have $n + q - 1 = 8 = 2 \cdot 4$, recovering the example (9.1). When $n = 6$, we have $n + q - 1 = 9 = 1 + 2 \cdot 4$, and when $n = 7$, we have $n + q - 1 = 10 = 2 \cdot 5$. □

10. Realizing symmetric n-linear forms by combinatorial polarization

We now describe symmetric n-linear forms that can be realized by polarization.

Lemma 10.1. *Let $\alpha : V \to F$ be a form and $n \geq 1$. Then $\alpha_n : V^n \to F$ is characteristic.*

Proof. There is nothing to prove when $n < \mathrm{char}(F)$. Assume that $n \geq p = \mathrm{char}(F) < \infty$ and let u, v_1, $\dots$, $v_{n-p} \in V$. Then

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

by the definition of α_n. Since p divides $\binom{p}{k}$ unless $k = 0$ or $k = p$, the inner sum reduces to

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

because $pu = 0$. 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 $2\alpha(v_{i_1} + \cdots + v_{i_r}) = 0$. □

On the other hand, every characteristic symmetric n-linear form φ is the nth derived form of some $\alpha : V \to F$, as we are going to show. In fact, we can demand that α be a totally reduced homogeneous polynomial. The idea is to set $\alpha(u) = \varphi(n * u)/n!$. We will first cover the case $n < \mathrm{char}(F)$, and then show how to work around the difficulty with the invertibility of $n!$ when $n \geq \mathrm{char}(F)$.

Lemma 10.2. *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, $\dots$, 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, $\dots$, u_m and integers $0 < s_1$, $\dots$, s_m, where $s_1 + \cdots + s_m = n$. Then $u_i \neq 0$ for every i by additivity. Moreover, $s_i < \mathrm{char}(F)$ since both φ, ψ are characteristic. Thus $v_1 = u_1$, $v_2 = 2u_1$, $\dots$, $v_{s_1} = s_1 u_1$, $v_{s_1+1} = u_2$, $\dots$, $v_{s_1+s_2} = s_2 u_2$, $\dots$, $v_n = s_m u_m$ are n distinct vectors. Then

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

a contradiction. □

Lemma 10.3. *Let $n < \mathrm{char}(F)$, and let $\varphi : V^n \to F$ be a symmetric n-additive form. Then $\alpha : V \to F$ defined by*

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

satisfies $\alpha_n = f$.

Proof. Both α_n and φ are characteristic since $n < \mathrm{char}(F)$. By Lemma 10.2, it suffices to show that $\alpha_n(u_1, \dots, u_n) = \varphi(u_1, \dots, u_n)$ for every pairwise distinct vectors $u_1, \dots, u_n$ of V. We have

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

Let $v_1, \dots, v_m$ be pairwise distinct vectors of V such that $\{v_1, \dots, v_m\} \subseteq \{u_1, \dots, u_n\}$, and let $1 \le s_i \le n$ be such that $s_1 + \dots + s_m = n$. We count how many times $\varphi(s_1 * v_1, \dots, s_m * v_m)$ appears in $\alpha_n(u_1, \dots, u_n)$. It appears precisely in those summands $\varphi(n * (u_{i_1} + \dots + u_{i_k}))$ 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 k, there are precisely $\binom{n-m}{k}$ subsets $\{u_{i_1}, \dots, u_{i_{k+m}}\}$ containing $\{v_1, \dots, v_m\}$. Altogether, $\varphi(s_1 * v_1, \dots, s_m * v_m)$ appears

$$\binom{n}{s_1, \dots, s_m} \sum_{k=0}^{n-m} (-1)^{n-(k+m)} \binom{n-m}{k} \tag{10.1}$$

times. Recall that

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

Hence (10.1) vanishes when $m < n$. When $m = n$, we have $s_1 = \dots = s_n = 1$, and so (10.1) is equal to $n!$. □

Let $\{e_1, \dots, e_d\}$ be a basis of V and $\varphi : V^n \to F$ a symmetric n-linear form. Then

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

When φ is characteristic (and this is the only interesting case by Lemma 10.1), the formula becomes

$$\varphi\left(n * \sum_{i=1}^{d} a_i e_i\right) = \sum_{0 \le t_i < \mathrm{char}(F),\ t_1 + \dots + t_d = n} \binom{n}{t_1, \dots, t_d} a_1^{t_1} \cdots a_d^{t_d} \varphi(t_1 * e_1, \dots, t_d * e_d). \tag{10.2}$$

If $n < p = \mathrm{char}(F)$, we can divide by $n!$ and proceed as in Lemma 10.3. When $n = p$, (10.2) is equal to 0, since φ is characteristic. In fact, every summand in (10.2) is equal to zero, since the multinomial coefficient $\binom{n}{t_1, \dots, t_d}$ is equal to zero. However, it is important to note that the multiplicity of p in the prime factorization of $\binom{n}{t_1, \dots, t_d}$ is the same as the multiplicity of p in the prime factorization of n. It is therefore possible to "divide" the right hand side of (10.2), and recover some information about φ. Formally:

Theorem 10.4 (Realization)**.** *Let $B = \{e_1, \dots, e_d\}$ be a basis of V and $\varphi : V^n \to F$ a characteristic symmetric n-linear form. Let $p = \mathrm{char}(F) \le \infty$. Write $n! = p^m \cdot r$, where $(p, r) = 1$. Define $\alpha : V \to F$ by*

$$\alpha(\sum a_i e_i) = \frac{1}{r} \cdot \sum_{0 \le t_i < p,\ t_1 + \dots + t_d = n} \frac{\binom{n}{t_1, \dots, t_d}}{p^m} a_1^{t_1} \cdots a_d^{t_d} \varphi(t_1 * e_1, \dots, t_d * e_d),$$

where by

$$\frac{\binom{n}{t_1, \dots, t_d}}{p^m} \tag{10.3}$$

we mean the integer $\binom{n}{t_1, \dots, t_d}$ divided by the integer p^m, and only then considered as an element of the prime field of F.

Then $\alpha_n = \varphi$, $\mathrm{cdeg}(\alpha) \le n$, and $\alpha(au) = a^n \alpha(u)$ for every $a \in F$, $u \in V$. Moreover, α is a totally reduced homogeneous polynomial of degree n.

Proof. By the discussion above, the number (10.3) is an integer that is relatively prime to p. Then the proof of Lemma 10.3 goes through word for word, showing $\alpha_n = \varphi$. Since φ is n-additive, $\mathrm{cdeg}(\alpha) \le n$. Clearly, $\alpha(au) = a^n \alpha(u)$, α is totally reduced, and homogeneous of degree n. □

Example 10.5 ($n = p = 3$)**.** 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 $u = a_1 e_1 + a_2 e_2 + a_3 e_3$. Then

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

Since the multiplicity of 3 in the prime factorization of 3! is 1, the formula for α from Theorem 10.4 becomes

$$\alpha(u) = \frac{1}{2} \left(\sum_{i \ne j} a_i^2 a_j \varphi(e_i, e_i, e_j) + \sum_{i<j<k} 2 a_i a_j a_k \varphi(e_i, e_j, e_k) \right).$$

11. Characteristic n-linear forms

One of the intentions of this paper is to demonstrate that characteristic symmetric n-linear forms are related to forms of degree n by polarization in a way that can be understood as a natural generalization of the relationship between alternating bilinear forms and quadratic forms. We have shown in Theorem 10.4 that all characteristic n-linear forms (i.e., all elements of $\mathrm{CharF}(V, n) \cap \mathrm{LinF}(V, n)$) can be obtained by polarizing a polynomial form of degree n. In Section 9 we have shown that polynomial forms of degree n correspond to totally reduced homogeneous polynomials of degree n modulo some monomials of smaller p-degree. We shall now put these two results together to establish the following one-to-one correspondence:

Theorem 11.1 (Characteristic n-linear forms)**.** *For every $n \ge 1$ we have*

$$\mathrm{CharF}(V, n) \cap \mathrm{LinF}(V, n) \cong \mathrm{Pol}_{tot}(V, n)/(\mathrm{Pol}_{tot}(V, n) \cap \mathrm{Pol}(V, n-1))$$

as vector spaces. In words, characteristic n-linear forms over a d-dimensional vector space are in one-to-one correspondence with totally reduced homogeneous polynomials of (combinatorial) degree n in d variables.

Proof. For a polynomial map $\alpha : V \to F$ with $\mathrm{cdeg}(\alpha) \le n$, let $\omega(\alpha) = \alpha_n$. When $\alpha \in \mathrm{Pol}_{tot}(V, n)$, $\omega(\alpha)$ is n-linear, by Proposition 9.2. Also, $\omega(\alpha)$ is characteristic by Lemma 10.1. Hence, upon restricting ω to $\mathrm{Pol}_{tot}(V, n)$, we can consider it as a map

$\mathrm{Pol}_{tot}(V,n) \to \mathrm{CharF}(V,n) \cap \mathrm{LinF}(V,n)$. Combinatorial polarization is linear, and thus ω is a homomorphism. Clearly, $\ker(\omega) = \mathrm{Pol}_{tot}(V,n) \cap \mathrm{Pol}(V,n-1)$. It remains to show that ω is onto. But this follows from Theorem 10.4.

The degree and combinatorial degree coincide for totally reduced polynomials. $\square$

Corollary 11.2. *The vector space* $\mathrm{CharF}(V,n) \cap \mathrm{LinF}(V,n)$ *has dimension equal to the number of integral solutions* $(x_1,\dots,x_d)$ *to the equation* $x_1 + \cdots + x_d = n$*, subject to the constraints* $0 \le x_i < \mathrm{char}(F)$*. In particular,* $\mathrm{CharF}(V,n) \cap \mathrm{LinF}(V,n) = 0$ *if* $d(\mathrm{char}(F) - 1) < n$*.*

The correspondence takes on a particulary simple form when $\mathrm{char}(F) = \infty$:

Corollary 11.3. *Let* $d \ge 1$*,* V *a* d*-dimensional vector space over* F*, and* $\mathrm{char}(F) = \infty$*. Then homogeneous polynomials of degree* n *in* d *variables are in one-to-one correspondence with symmetric* n*-linear forms* $V \to F$*.*

Proof. When $\mathrm{char}(F) = \infty$, we have $\mathrm{CharF}(V,n) \cap \mathrm{LinF}(V,n) = \mathrm{LinF}(V,n)$, and all polynomials are totally reduced. Factoring out polynomials of degree at most $n-1$ leaves homogeneous polynomials of degree n. $\square$

12. When are forms of degree n polynomial, and other open questions

Let us return to the question whether forms of degree n are necessarily polynomial maps. The answer is positive over finite fields, by Theorem 3.3. Corollary 12.3 gives a partial answer for arbitrary fields:

Lemma 12.1. *Let* $n > 0$*,* $s > 0$*. The number of words of length* s *containing all letters of an* n*-letter alphabet is equal to*

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^s.$$

In particular,

$$\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n = n!.$$

Proof. There are n^s words of length s formed from an n-letter alphabet. All words of length s omitting at least one letter are obtained as follows: select $n-1$ letters and form a word of length s using the letters. This can be done in $\binom{n}{n-1}(n-1)^s$ ways. But some words are counted more than once, namely those missing at least two letters. The formula then follows from the inclusion-exclusion principle.

When $s = n$, the words containing all letters are precisely the permutations of the n-letter alphabet. $\square$

Lemma 12.2. *Let* F *be a field of characteristic bigger than* n*, and let* $\alpha : V \to F$ *be a map satisfying* $\mathrm{cdeg}(\alpha) < n$*,* $\alpha(au) = a^n \alpha(u)$*. Then* $\alpha = 0$*.*

Proof. Let $u \in V$. We have

$$0 = \alpha_n(n * u) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \alpha(ku) = \alpha(u) \cdot \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n.$$

Thus, by Lemma 12.1, $0 = \alpha(u) \cdot n!$. Since $n < \mathrm{char}(F)$, we have $\alpha(u) = 0$. $\square$

Corollary 12.3. *Let* $\alpha : V \to F$ *be a form of degree* n*, and assume that* $\mathrm{char}(F) > n$*. Then* α *is a polynomial map. In fact,* α *is the polynomial of Theorem* 10.4*.*

Proof. Let β be the polynomial of Theorem 10.4. Then $\beta_n = \alpha_n$, and thus $\gamma = \alpha - \beta$ is a map satisfying $\mathrm{cdeg}(\gamma) < n$ and $\gamma(au) = a^n\gamma(u)$. By Lemma 12.2, $\gamma = 0$. □

Incidentally, we can now sharpen Corollary 9.4 as follows:

Corollary 12.4. *Let $n \geq 1$, and let V be a vector space over a field F of characteristic ∞. Then the vector space of forms $\alpha : V \to F$ of degree n is isomorphic to the vector space of homogeneous polynomials of degree n.*

We ask:

Problem 12.5. *Is every form of degree n a polynomial map?*

Given a form α of degree n, there exists a polynomial form β of degree n such that $\alpha_n = \beta_n$, by Theorem 10.4. Thus $\gamma = \alpha - \beta$ satisfies $\gamma(au) = a^n\gamma(u)$ and $\mathrm{cdeg}(\gamma) = m < n$. Whence, if Problem 12.6 is answered affirmatively, so is Problem 12.5.

Problem 12.6. *Let $\alpha : V \to F$ be a map satisfying $\alpha(au) = a^n\alpha(u)$ and $\mathrm{cdeg}(\alpha) = m < n$. Is α a polynomial map?*

Here are some remarks concerning Problem 12.6.

(a) The condition $\alpha(au) = a^n\alpha(u)$ is necessary. To see this, consider a basis B of $\mathbb{R}$ over $\mathbb{Q}$, and define $\alpha : B \to \mathbb{Q}$ arbitrarily but so that $\alpha(u) \neq 0$ for infinitely many $u \in B$, and $\alpha \neq 0$. Extend α uniquely into a homomorphism $\alpha : \mathbb{R} \to \mathbb{Q}$, and consider it as a map $\alpha : \mathbb{R} \to \mathbb{R}$. Then $\mathrm{cdeg}(\alpha) = 1$, but α is not a polynomial (in one variable) since it has too many zeros.

(b) We can assume that $d = \dim(V) > 1$. Otherwise $\alpha : V = F \to F$ satisfies $\alpha(a1) = a^n\alpha(1)$, and thus it is a polynomial map with respect to the basis $B = \{1\}$.

(c) We can assume that $n \equiv m \pmod{p-1}$. Suppose that $n \not\equiv m \pmod{p-1}$, and let $u_1, \dots, u_m \in V$ be such that $\alpha_m(u_1, \dots, u_m) \neq 0$. Let a be a generator of the multiplicative group of the prime field of F. On the one hand, we have $\alpha_m(au_1, \dots, au_m) = a^m\alpha_m(u_1, \dots, u_m)$ because α_m is m-additive. On the other hand, the definition of α_m together with the condition $\alpha(au) = a^n\alpha(u)$ imply $\alpha_m(au_1, \dots, au_m) = a^n\alpha_m(u_1, \dots, u_m)$. Hence $a^n = a^m$, a contradiction.

(d) We can assume that $\omega_p(n) \leq m$. Suppose that $\omega_p(n) > m$, and consider the map $\delta : F \to F$, $a \mapsto a^n$. Then $\mathrm{cdeg}(\delta) = \omega_p(n) > m$, thus $\delta_{m+1} \neq 0$, so δ_m is not m-additive. Let $v \in V$ be such that $\alpha(v) \neq 0$. By the definition of α_m, we have $\alpha_m(a_1v, \dots, a_mv) = \delta_m(a_1, \dots, a_m)\alpha(v)$, and so α_m is not m-additive either.

We can now restate Problem 12.6 with more details:

Let F be a field of characteristic $p = \mathrm{char}(F)$. Let $\alpha : V \to F$ be a map satisfying $\alpha(au) = a^n\alpha(u)$ and $\mathrm{cdeg}(\alpha) = m < n$. Assume that $\dim(V) > 1$, $n \equiv m \pmod{p-1}$, and $\omega_p(n) \leq m$. Is α a polynomial map?

In particular, is α a polynomial map when $\dim(V) = 2$, $p = 2$, $n = 3$, and $m = 2$?

Finally, returning to Proposition 9.5, we pose:

Problem 12.7. *Characterize all pairs (V, n) for which $\mathrm{Pol}_{tot}(V, n) \cap \mathrm{Pol}_{\equiv}(V, n)$ does contain only homogeneous polynomials of degree n.*

References

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

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

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

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

[5] 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.
[6] Harold N. Ward, *Combinatorial polarization*, Discrete Math. **26** (1979), no. **2**, 185–197.

(Drápal) Department of Algebra, Charles University, Sokolovská 183, Praha 186 75, Czech Republic
E-mail address: `drapal@karlin.mff.cuni.cz`

(Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, U.S.A.
E-mail address: `petr@math.du.edu`