COMBINATORIAL POLARIZATION, CODE LOOPS, AND CODES OF HIGH LEVEL

PETR VOJTĚCHOVSKÝ

We first find the combinatorial degree of any map $f : V \to F$, where F is a finite field and V is a finite-dimensional vector space over F. We then simplify and generalize a certain construction, due to Chein and Goodaire, that was used in characterizing code loops as finite Moufang loops that possess at most two squares. The construction yields binary codes of high divisibility level with prescribed Hamming weights of intersections of codewords.

2000 Mathematics Subject Classification: 20N05, 05A10.

1. Introduction. Let V be a finite-dimensional vector space over F. Given a map $f : V \to F$, the *nth derived form* $\delta_n f : V^n \to F$ is defined by

$$\delta_n f(v_1, \ldots, v_n) = \sum (-1)^{n-m} f(v_{i_1} + \cdots + v_{i_m}), \tag{1.1}$$

where the summation runs over all subsets of $\{v_1, \ldots, v_n\}$, where we consider v_i different from v_j if $i \neq j$. We have borrowed the name "derived form" from [1, page 41]. The process of obtaining the forms $\delta_n f$ from f is referred to as *combinatorial polarization*. It can also be described recursively by the formula

$$\begin{aligned}
\delta_{n+1} f(v_1, \ldots, v_{n+1}) &= \delta_n f(v_1 + v_2, v_3, \ldots, v_{n+1}) - \delta_n f(v_1, v_3, \ldots, v_{n+1}) \\
&\quad - \delta_n f(v_2, v_3, \ldots, v_{n+1})
\end{aligned} \tag{1.2}$$

for $v_1, \ldots, v_{n+1} \in V$.

The *combinatorial degree* cdeg f of f is the smallest nonnegative integer n such that $\delta_m f = 0$ for every $m > n$, if it exists, and it is equal to ∞ otherwise. Note that the combinatorial degree of the zero map is 0.

Combinatorial polarization was first studied by Ward in [6]. He shows in [6, Proposition 2.8] that the combinatorial degree of a polynomial map is equal to its degree if F is a prime field or a field of characteristic 0, and he remarks that "It is not difficult to show that, in general, the combinatorial degree of a nonzero polynomial over $\mathrm{GF}(q)$, 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 polynomials" [6, Page 195]. Since he does not prove the statement and since the author believes that the proof is not absolutely trivial, we offer it in Section 2. We then move on to code loops and codes of high level.

Recall that *loop* is a groupoid $(L, \cdot)$ with neutral element 1 such that the equation $x \cdot y = z$ has a unique solution whenever two of the three elements $x, y, z \in L$ are

specified. The variety of loops defined by the identity $x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z$ is known as *Moufang loops*. The *commutator* $[x,y]$ of $x,y \in L$ is the unique element $u \in L$ such that $xy = (yx)u$. Similarly, the *associator* $[x,y,z]$ of $x,y,z \in L$ is the unique element $u \in L$ such that $(xy)z = (x(yz))u$.

We will need basic terminology from coding theory. A (linear) *code* C is a subspace of V. For every *codeword* $c = (c_1,\ldots,c_m) \in C$, we define its (Hamming) *weight* $w(c)$ as the number of nonzero coordinates c_i in c. If 2^r divides $w(c)$ for every $c \in C$ and if r is as big as possible, then C is said to be of *level* r.

Codes of level 2 are usually called *doubly even*, and doubly even codes are behind Griess' definition of a code loop. Let C be a doubly even code over $F = \{0,1\}$ and let $\eta : C \times C \to F$ be such that

$$
\begin{aligned}
\eta(x,x) &= \frac{w(x)}{4}, \\
\eta(x,y) + \eta(y,x) &= \frac{w(x \cap y)}{2}, \\
\eta(x,y) + \eta(x+y,z) + \eta(y,z) + \eta(x,y+z) &= w(x \cap y \cap z),
\end{aligned}
\tag{1.3}
$$

for every $x,y,z \in C$. (Here, $x \cap y$ is the vector whose ith coordinate is equal to 1 if and only if the ith coordinates of both x and y are equal to 1.) Then $L = C \times F$, with multiplication

$$
(x,a)(y,b) = (x+y, a+b+\eta(x,y)),
\tag{1.4}
$$

is a *code loop* for C. Griess shows in [4] that there is a unique code loop for C, up to isomorphism, and that it is Moufang.

Chein and Goodaire found a nice characterization of code loops. Namely, they show that code loops are exactly finite Moufang loops with at most two squares (cf. [2, Theorem 5]). Their proof is based on three observations.

First, if L is a Moufang loop with $|L^2| \leq 2$, then every commutator and associator belong to L^2 and

$$
\begin{aligned}
(xy)^2 &= x^2 y^2 [x,y], \\
[xy,z] &= [x,z][y,z][x,y,z], \\
[vx,y,z] &= [v,y,z][x,y,z]
\end{aligned}
\tag{1.5}
$$

hold for every $v,x,y,z \in L$ (see [2, Theorems 1, 2]). In other words, if we set $Z = L^2$, then L/Z is an elementary abelian 2-group, and the well-defined map $P : L/Z \to Z$, $x \mapsto x^2$, satisfies $\delta_2 P(x,y) = [x,y]$, $\delta_3 P(x,y,z) = [x,y,z]$, $\operatorname{cdeg} P = 3$, as can be seen immediately from (1.2) and (1.5). Note that under these circumstances, L is an elementary abelian 2-group if and only if $|L^2| = 1$.

Second, if $L = C \times F$ is a code loop for C and $x = (\tilde{x}, a)$, $y = (\tilde{y}, b)$, and $z = (\tilde{z}, c)$ belong to L, then

$$x^2 = \left(0, \frac{w(\tilde{x})}{4}\right),$$

$$[x, y] = \left(0, \frac{w(\tilde{x} \cap \tilde{y})}{2}\right), \tag{1.6}$$

$$[x, y, z] = (0, w(\tilde{x} \cap \tilde{y} \cap \tilde{z}))$$

by [2, Lemma 6]. (Note that (1.5) then holds because $w(u + v) = w(u) + w(v) - 2w(u \cap v)$ for any two binary vectors u, v.)

Third, given an integer $n \geq 1$ and parameters $\alpha_i, \beta_{ij}, \gamma_{ijk} \in \{0, 1\}$, for $1 \leq i, j, k \leq n$, there is a doubly even code C with basis $c_1, \dots, c_n$ such that

$$\alpha_i = w(c_i),$$

$$\beta_{ij} = w(c_i \cap c_j), \tag{1.7}$$

$$\gamma_{ijk} = w(c_i \cap c_j \cap c_k),$$

for $1 \leq i, j, k \leq n$ (cf. the proof of [2, Theorem 5]). It is this construction that turns out to be the most difficult part of the proof that code loops are exactly finite Moufang loops with at most two squares. We simplify and generalize the construction in Section 3. The construction presented here is easier than that of [5] too, because it avoids induction.

To conclude our discussion concerning code loops, note that a map $f : V \to \{0, 1\}$ with combinatorial degree 3 is uniquely specified if we know the values of $f(e_i)$, $f(e_i + e_j)$, and $f(e_i + e_j + e_k)$ for some basis $e_1, \dots, e_n$ of V. Hence, by (1.5), (1.6), and (1.7), code loops can be identified with maps $P : V \to \{0, 1\}$ of combinatorial degree 3.

2. Combinatorial degree over finite fields. In this section, let V be a vector space of dimension n over the field $F = \mathrm{GF}(q)$ of characteristic p and let $f : V \to F$ be an arbitrary map.

By an easy generalization of the fundamental theorem of algebra, we can identify f with some polynomial in $F[x_1, \dots, x_n]$. Moreover, if we assume that the polynomial is *reduced*, then it is unique. Here is what we mean by reduced polynomial: if $cx_1^{a_1} \cdots x_n^{a_n}$ is a monomial of f, then $0 \leq a_i < q$, for $1 \leq i \leq n$, and if $cx_1^{a_1} \cdots x_n^{a_n}$, $dx_1^{b_1} \cdots x_n^{b_n}$ are two such monomials of f, we must have $a_i \neq b_i$ for some $1 \leq i \leq n$.

We will assume from now on that f is a reduced polynomial. We write $\mathbf{x}$ for $(x_1, \dots, x_n)$ and $\mathbf{x^a}$ for $x_1^{a_1} \cdots x_n^{a_n}$. Then

$$f(\mathbf{x}) = \sum_{\mathbf{a} \in M(f)} c_{\mathbf{a}} \mathbf{x^a}, \tag{2.1}$$

where $M(f)$ is the set of all multiexponents of f, and $0 \neq c_{\mathbf{a}} \in F$ for every $\mathbf{a} \in M(f)$.

Our goal is to calculate the combinatorial degree of f. When $f(0) \neq 0$, then $\mathrm{cdeg}\, f = \infty$ by (1.2). We will therefore assume that $f(0) = 0$ from now on.

LEMMA 2.1. *Let $f : V \to F$ be as in (2.1). Then*

$$\operatorname{cdeg} f = \max \left\{ \operatorname{cdeg} \mathbf{x}^{\mathbf{a}}; \ \mathbf{a} \in M(f) \right\}. \tag{2.2}$$

PROOF. We call two polynomials f, g *disjoint* if $M(f) \cap M(g) = \varnothing$. Since every polynomial is a sum of monomials, it suffices to prove that if two monomials are disjoint, then their derived forms are disjoint too.

To see this, consider the monomial $g(\mathbf{x_1}) = \mathbf{x_1}^{\mathbf{a}}$, where $\mathbf{x_1} = (x_{11}, \dots, x_{1n})$, $\mathbf{a} = (a_1, \dots, a_n)$. As seen in (1.1), a typical summand of $\delta_r g$ is $h = g(\mathbf{x_1} + \cdots + \mathbf{x_r})$, which is a polynomial in nr variables. The crucial observation is that for every $1 \le j \le r$, every monomial of h contains exactly a_i variables x_{ji}, with possible repetitions. Hence the original monomial $\mathbf{x_1}^{\mathbf{a}}$ can be uniquely reconstructed from every monomial of h. □

We focus on reduced monomials from now on. When $\mathbf{a} = (a_1, \dots, a_n)$, $\mathbf{b} = (b_1, \dots, b_n)$ are two multiexponents, we write $\mathbf{a} \le \mathbf{b}$ if $a_i \le b_i$ for every $1 \le i \le n$, and $\mathbf{a} < \mathbf{b}$ if $\mathbf{a} \le \mathbf{b}$, and there is $1 \le i \le n$ with $a_i < b_i$.

LEMMA 2.2. *Let $f(\mathbf{x}) = \mathbf{x}^{\mathbf{a}}$. Then*

$$\delta_2 f(\mathbf{x}, \mathbf{y}) = \sum_{0 < \mathbf{b} < \mathbf{a}} c_{\mathbf{a}, \mathbf{b}} \mathbf{x}^{\mathbf{b}} \mathbf{y}^{\mathbf{a} - \mathbf{b}}, \tag{2.3}$$

where

$$c_{\mathbf{a}, \mathbf{b}} = \prod_{i=1}^{n} \binom{a_i}{b_i}. \tag{2.4}$$

More generally, if $f(\mathbf{x_1}) = \mathbf{x_1}^{\mathbf{a_1}}$, then

$$
\begin{aligned}
&\delta_s f(\mathbf{x_1}, \dots, \mathbf{x_s}) \\
&= \sum_{0 < \mathbf{a_2} < \mathbf{a_1}} \cdots \sum_{0 < \mathbf{a_s} < \mathbf{a_{s-1}}} c_{\mathbf{a_1}, \mathbf{a_2}} \cdots c_{\mathbf{a_{s-1}}, \mathbf{a_s}} \mathbf{x_1}^{\mathbf{a_s}} \mathbf{x_2}^{\mathbf{a_{s-1}} - \mathbf{a_s}} \cdots \mathbf{x_s}^{\mathbf{a_1} - \mathbf{a_2}},
\end{aligned} \tag{2.5}
$$

where $c_{\mathbf{a_i}, \mathbf{a_{i+1}}}$ is analogous to (2.4).

PROOF. We have

$$
\begin{aligned}
(\mathbf{x} + \mathbf{y})^{\mathbf{a}} &= \prod_{i=1}^{n} (x_i + y_i)^{a_i} = \prod_{i=1}^{n} \sum_{b_i=0}^{a_i} \binom{a_i}{b_i} x_i^{b_i} y_i^{a_i - b_i} \\
&= \sum_{b_1, \dots, b_n, 0 \le b_i \le a_i} \left(\prod_{i=1}^{n} \binom{a_i}{b_i} x_i^{b_i} y_i^{a_i - b_i} \right) \\
&= \sum_{b_1, \dots, b_n, 0 \le b_i \le a_i} \left(\prod_{i=1}^{n} \binom{a_i}{b_i} \right) x_1^{b_1} \cdots x_n^{b_n} y_1^{a_1 - b_1} \cdots y_n^{a_n - b_n}.
\end{aligned} \tag{2.6}
$$

Since $\delta f(\mathbf{x}, \mathbf{y}) = (\mathbf{x} + \mathbf{y})^{\mathbf{a}} - \mathbf{x}^{\mathbf{a}} - \mathbf{y}^{\mathbf{a}}$, we are done with (2.3).

We have also proved the more general statement (2.5) for $s = 2$, and we proceed by induction on s. Assume that (2.5) holds for s. Using the polarization formula (1.2) on

every summand of (2.5), we see that $\delta_{s+1}f(\mathbf{x_1},\ldots,\mathbf{x_{s+1}})$ is equal to

$$\sum_{0<\mathbf{a_2}<\mathbf{a_1}}\cdots\sum_{0<\mathbf{a_s}<\mathbf{a_{s-1}}} c_{\mathbf{a_1},\mathbf{a_2}}\cdots c_{\mathbf{a_{s-1}},\mathbf{a_s}}\delta_2 g(\mathbf{x_1},\mathbf{x_2})\mathbf{x_3}^{\mathbf{a_{s-1}}-\mathbf{a_s}}\cdots\mathbf{x_{s+1}}^{\mathbf{a_1}-\mathbf{a_2}}, \tag{2.7}$$

where $g(\mathbf{x}) = \mathbf{x^{a_s}}$. The term $\delta_2 g(\mathbf{x_1},\mathbf{x_2})$ expands as

$$\sum_{0<\mathbf{a_{s+1}}<\mathbf{a_s}} c_{\mathbf{a_s},\mathbf{a_{s+1}}}\mathbf{x_1}^{\mathbf{a_{s+1}}}\mathbf{x_2}^{\mathbf{a_s}-\mathbf{a_{s+1}}} \tag{2.8}$$

by (2.3), and we are done. $\square$

Let $\mathbf{a} = (a_1,\ldots,a_n)$ be a multiexponent, $f(\mathbf{x}) = \mathbf{x^a}$. Lemma 2.1 shows that $\delta_s f$ is not the zero map if and only if there is a chain of multiexponents $\mathbf{a} = \mathbf{a_1} > \mathbf{a_2} > \cdots > \mathbf{a_s}$ such that $c_{\mathbf{a_i},\mathbf{a_{i+1}}}$ does not vanish in F for every $1 \le i < s$. We will call such chains of multiexponents *regular* here. Obviously, the length of a regular chain is bounded by q^n.

LEMMA 2.3. *Let $\mathbf{a_i} = (a_{i1},\ldots,a_{in})$ for $1 \le i \le s$. Assume that $\mathbf{a_1} > \cdots > \mathbf{a_s}$ is a regular chain of maximum length for $\mathbf{a_1}$. Then $\mathbf{a_{i+1}}$, $\mathbf{a_i}$ differ in exactly one position, that is, $a_{i+1,j} \ne a_{ij}$ for a unique $1 \le j \le n$.*

PROOF. Suppose that there are $1 \le i < s$ and $1 \le j < k \le n$ such that $a_{i+1,j} \ne a_{ij}$ and $a_{i+1,k} \ne a_{ik}$. Construct a multiexponent $\mathbf{b}$ so that

$$b_m = \begin{cases} a_{i,m}, & \text{if } m \ne j, \\ a_{i+1,m}, & \text{if } m = j. \end{cases} \tag{2.9}$$

Then $\mathbf{a_i} > \mathbf{b} > \mathbf{a_{i+1}}$. Since $c_{\mathbf{a_i},\mathbf{a_{i+1}}} = \prod_{m=1}^n \binom{a_{i,m}}{a_{i+1,m}} \ne 0$, we have $c_{\mathbf{a_i},\mathbf{b}} \ne 0$ and $c_{\mathbf{b},\mathbf{a_{i+1}}} \ne 0$. Thus $\mathbf{a_1},\ldots,\mathbf{a_i},\mathbf{b},\mathbf{a_{i+1}},\ldots,\mathbf{a_s}$ is a regular chain of length $s+1$, a contradiction. $\square$

COROLLARY 2.4. *Let $\mathbf{a} = (a_1,\ldots,a_n)$ be a multiexponent, $f(\mathbf{x}) = \mathbf{x^a}$, and $f_i(x) = x^{a_i}$, $1 \le i \le n$. Then*

$$\operatorname{cdeg} f = \sum_{i=1}^n \operatorname{cdeg} f_i. \tag{2.10}$$

We therefore continue to investigate combinatorial degrees of reduced monomials in one variable.

Let m be a positive integer. Then there are uniquely determined integers $0 \le m_i < p$ such that $m = \sum_{i=0}^\infty m_i p^i$. This p-adic expansion of m is useful when calculating binomial coefficients modulo p, as seen in the beautiful and still not so well-known theorem of Lucas (cf. [3]).

THEOREM 2.5 (Lucas theorem). *Let p be a prime and $m = \sum_{i=0}^\infty m_i p^i$, $k = \sum_{i=0}^\infty k_i p^i$ the p-adic expansions of m and k, respectively. Then*

$$\binom{m}{k} \equiv \prod_{i=0}^\infty \binom{m_i}{k_i} \pmod{p}, \tag{2.11}$$

where we set $\binom{a}{b} = 0$ whenever $a < b$.

The *p-weight* of $m = \sum_{i=0}^{\infty} m_i p^i$ is defined as $w_p(m) = \sum_{i=0}^{\infty} m_i$.

COROLLARY 2.6. *Let p be a prime and $a > 0$ an integer. Then the longest regular chain for a has length $w_p(a)$.*

PROOF. Let ℓ be the length of the longest regular chain for a. Theorem 2.5 shows that $\binom{m}{k} \not\equiv 0 \pmod{p}$ if and only if $m_i \geq k_i$ for every i (as both m_i, k_i are less than p, and $\binom{m_i}{k_i}$ with $m_i \geq k_i$ is therefore not divisible by p). This means that $w_p(m) \geq w_p(k)$ must be satisfied whenever $\binom{m}{k} \not\equiv 0 \pmod{p}$, and $\ell \leq w_p(a)$ follows.

On the other hand, if k is such that $k_i = m_i$, for each $i \neq j$, and $k_j = m_j - 1 \geq 0$, then $\binom{m}{k} \not\equiv 0 \pmod{p}$ by Theorem 2.5. Hence $\ell \geq w_p(a)$. $\square$

We have proved the following theorem.

THEOREM 2.7. *Let F be a finite field of characteristic p, let V be an n-dimensional vector space over F, and let $f : V \to F$ be a map. Then $f : V \to F$ can be written as a reduced polynomial $f(\mathbf{x}) = \sum_{\mathbf{a} \in M(f)} \mathbf{x}^{\mathbf{a}}$ in $F[\mathbf{x}]$, where $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{a} = (a_1, \ldots, a_n)$, and $M(f)$ is the set of all multiexponents of f. Moreover,*

$$\text{cdeg} f = \begin{cases} 0, & \text{if } f \text{ is the zero map,} \\ \infty, & \text{if } f(0) \neq 0, \\ \deg_p f, & \text{otherwise,} \end{cases} \tag{2.12}$$

where the p-degree $\deg_p f$ of f is calculated as

$$\deg_p f = \max_{(a_1, \ldots, a_n) \in M(f)} \sum_{i=1}^{n} w_p(a_i), \tag{2.13}$$

where the p-weight $w_p(a_i)$ of $a_i = \sum_{j=0}^{\infty} a_{ij} p^j$, $0 \leq a_{ij} < p$, is the integer

$$w_p(a_i) = \sum_{j=0}^{\infty} a_{ij}. \tag{2.14}$$

When F is a prime field, $\deg_p f = \deg f$.

EXAMPLE 2.8. Let $F = \text{GF}(9)$, $V = F^3$, and $f(x_1, x_2, x_3) = f_1(x_1, x_2, x_3) + f_2(x_1, x_2, x_3)$, where $f_1(x_1, x_2, x_3) = x_1^3 x_2^7$ and $f_2(x_1, x_2, x_3) = x_1 x_2 x_3^5$. Since $3 = 1 \cdot 3^1$, $7 = 1 \cdot 3^0 + 2 \cdot 3^1$, $1 = 1 \cdot 3^0$, and $5 = 2 \cdot 3^0 + 1 \cdot 3^1$, we have $w_3(3) = 1$, $w_3(7) = 1 + 2 = 3$, $w_3(1) = 1$, and $w_3(5) = 2 + 1 = 3$. Thus $\text{cdeg} f_1 = 1 + 3 = 4$, $\text{cdeg} f_2 = 1 + 1 + 3 = 5$, and $\text{cdeg} f = \max\{4, 5\} = 5$.

3. Codes of high level with prescribed weights of intersections of codewords. We will assume from now on that $F = \{0, 1\}$ is the two-element field and that V is a vector space over F of dimension n.

In the introduction, we have discussed a construction due to Chein and Goodaire that is used in characterizing code loops as finite Moufang loops with at most two squares. The fact that the values α_i, β_{ij}, γ_{ijk} in (1.7) can be prescribed can be restated as follows.

PROPOSITION 3.1 (Chein and Goodaire). *Let $P : V \to F$ be a map with $\operatorname{cdeg} P = 3$. Then there is a doubly even code C isomorphic to V such that $P(c) \equiv w(c)/4 \pmod 2$ for every $c \in C$.*

The original proof of this proposition is somewhat involved, and presents the biggest obstacle when characterizing code loops. We offer a simpler proof while at the same time generalizing the result to codes of arbitrary level.

THEOREM 3.2. *Let V be an n-dimensional vector space over $F = \{0,1\}$ and let $P : V \to F$ be such that $\operatorname{cdeg} P = r + 1$. Then there is a binary code C isomorphic to V and of level r such that $P(c) \equiv w(c)/2^r \pmod 2$ for every $c \in C$.*

PROOF. The map P can be identified with some polynomial in $F[x_1,\ldots,x_n]$. Calculating in $F[x_1,\ldots,x_n]$, we have

$$\prod_{i \in I} x_i = \sum_{K \in \mathcal{K}} \left(1 + \prod_{j \in K} (1 + x_j)\right), \tag{3.1}$$

where I is a subset of $\{1,\ldots,n\}$ and $\mathcal{K}$ is some set of subsets of I. Therefore

$$P(x_1,\ldots,x_n) = \sum_{J \in \mathcal{J}} \left(1 + \prod_{j \in J} (1 + x_j)\right) \tag{3.2}$$

for some set $\mathcal{J}$ of subsets of $\{1,\ldots,n\}$.

Let H be the parity-check matrix of the Hamming code of dimension $r + 1$ (and length $2^{r+1} - 1$). Hence the rows of H are exactly the nonzero vectors of F^{r+1} in some order. Let D be the code whose generating matrix is the transpose of H. Then $w(d) = 2^r$ for every nonzero $d \in D$. Every codeword d can be written as a linear combination of columns of H, and hence identified with some $(d_1,\ldots,d_{r+1}) \in F^{r+1}$. Note that

$$\frac{w(d)}{2^r} \equiv 1 + \prod_{i=1}^{r+1} (1 + d_i) \tag{3.3}$$

since the product $\prod_{i=1}^{r+1} (1 + d_i)$ vanishes for every nonzero $d \in D$.

For every subset $J = \{j_1,\ldots,j_t\}$ in $\mathcal{J}$, define the map $\pi_J : V \to D$ by

$$\pi_J(x_1,\ldots,x_n) = (x_{j_1},\ldots,x_{j_t},0,\ldots,0) \in F^{r+1}. \tag{3.4}$$

This map is well defined because $r + 1 = \operatorname{cdeg} P = \deg_2 P = \deg P = \max_{J \in \mathcal{J}} |J|$, by Theorem 2.7. For $x \in V$, let $\pi(x) = \bigoplus_{J \in \mathcal{J}} \pi_J(x)$ and let C be the image of V under π. Then C is isomorphic to V and, for $x = (x_1,\ldots,x_m) \in V$,

$$P(x) = \sum_{J \in \mathcal{J}} \left(1 + \prod_{j \in J} (1 + x_j)\right) \equiv \sum_{J \in \mathcal{J}} \frac{w(\pi_J(x))}{2^r} = \frac{w(\pi(x))}{2^r} \tag{3.5}$$

by (3.3). This finishes the proof. $\qquad\square$

We will work out an example illustrating the proof of Theorem 3.2.

EXAMPLE 3.3. Let $P : V = F^3 \to F$ be the map $P(x_1, x_2, x_3) = x_2 + x_1 x_3 + x_1 x_2 x_3$. Then

$$P(x_1, x_2, x_3) = (1 + x_1' x_2') + (1 + x_2' x_3') + (1 + x_1' x_2' x_3'), \tag{3.6}$$

where $x_i' = 1 + x_i$. Thus $\mathcal{J} = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$. We have $\operatorname{cdeg} P = \deg P = 3 = r + 1$ and $n = \dim V = 3$.

The construction depends on a choice of the (dual) Hamming code. We pick the code whose generating matrix is

$$H^T = \begin{pmatrix} 1000111 \\ 0101011 \\ 0011101 \end{pmatrix}. \tag{3.7}$$

The explicit construction also depends on an ordering of the elements of $\mathcal{J}$. We agree that they are listed as above. Then $\pi(x) = \pi_{\{1,2\}}(x) \oplus \pi_{\{2,3\}}(x) \oplus \pi_{\{1,2,3\}}(x)$.

Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, and $e_3 = (0, 0, 1)$ be the canonical basis for V. Then, with respect to the basis consisting of the three rows of H^T, the vectors e_1, e_2, and e_3 are mapped onto

$$\begin{aligned}
\pi(e_1) &= (1, 0, 0) \oplus (0, 0, 0) \oplus (1, 0, 0) = c_1, \\
\pi(e_2) &= (0, 1, 0) \oplus (1, 0, 0) \oplus (0, 1, 0) = c_2, \\
\pi(e_3) &= (0, 0, 0) \oplus (0, 1, 0) \oplus (0, 0, 1) = c_3.
\end{aligned} \tag{3.8}$$

For instance, the middle summand of c_3 is $(0, 1, 0)$ because $\pi_{\{2,3\}}(0, 0, 1) = (0, 1, 0)$.

Viewed as vectors over F, the vectors c_1, c_2, and c_3 (forming a basis of C) become

$$\begin{aligned}
c_1 &= (1000111, 0000000, 1000111), \\
c_2 &= (0101011, 1000111, 0101011), \\
c_3 &= (0000000, 0101011, 0011101).
\end{aligned} \tag{3.9}$$

We test Theorem 3.2 on two vectors. First, let $x = e_3$. Then $P(x) = 0 + 0 + 0 = 0$, $c = \pi(x) = c_3$, and $w(c)/2^2 = 8/4 = 2$. Similarly, with $x = e_1 + e_2 + e_3$, we obtain $P(x) = 1 + 1 + 1 = 1$,

$$c = \pi(x) = c_1 + c_2 + c_3 = (1101100, 1101100, 1110001), \tag{3.10}$$

and $w(c)/2^2 = 12/4 = 3$. In both cases, $w(c)/2^r \equiv P(x) \pmod 2$.

The construction of Theorem 3.2 allows us to calculate the dimension of the resulting code C over F.

COROLLARY 3.4. *Let P, C be as in Theorem 3.2,*

$$P(x_1, \ldots, x_n) = \sum_{J \in \mathcal{J}} \left(1 + \prod_{j \in J} (1 + x_j) \right). \tag{3.11}$$

Then the dimension of C over F is equal to $|\mathcal{J}| \cdot (2^{\deg P} - 1)$.

References

[1] M. Aschbacher, *Sporadic Groups*, Cambridge Tracts in Mathematics, vol. 104, Cambridge University Press, Cambridge, 1994.

[2] O. Chein and E. 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] R. L. Griess Jr., *Code loops*, J. Algebra **100** (1986), no. 1, 224–234.

[5] P. Vojtěchovský, *Combinatorial aspects of code loops*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 429–435.

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

Petr Vojtěchovský: Department of Mathematics, University of Denver, 2360 S. Gaylord Street, Denver, CO 80208, USA

E-mail address: petr@math.du.edu