

# GENERALIZED POLYNOMIALS AND HYPERPLANE FUNCTIONS IN $(\mathbb{Z}/p^k\mathbb{Z})^n$

IZABELLA LABA AND CHARLOTTE TRAINOR

ABSTRACT. For  $p$  prime, let  $\mathcal{H}^n$  be the linear span of characteristic functions of hyperplanes in  $(\mathbb{Z}/p^k\mathbb{Z})^n$ . We establish new upper bounds on the dimension of  $\mathcal{H}^n$  over  $\mathbb{Z}/p\mathbb{Z}$ , or equivalently, on the rank of point-hyperplane incidence matrices in  $(\mathbb{Z}/p^k\mathbb{Z})^n$  over  $\mathbb{Z}/p\mathbb{Z}$ . Our proof is based on a variant of the polynomial method using binomial coefficients in  $\mathbb{Z}/p^k\mathbb{Z}$  as generalized polynomials. We also establish additional necessary conditions for a function on  $(\mathbb{Z}/p^k\mathbb{Z})^n$  to be an element of  $\mathcal{H}^n$ .

## CONTENTS

1. Introduction	2
2. Relationships between incidence matrices	6
3. The binomial phi functions	9
3.1. Definitions	9
3.2. Properties of phi functions	11
4. Discrete derivatives	11
4.1. Definitions	11
4.2. More properties of phi functions	13
5. Phi functions on $R^n$	15
5.1. Phi functions as generalized polynomials	15
5.2. Phi functions and hyperplanes	18
6. Degree lowering for products	20
7. An upper bound on the rank of hyperplane functions	22
8. Geometric test for hyperplane functions	25
8.1. Preliminary lemmas	26
8.2. A simplified geometric test	28
8.3. Generalizing the geometric test	29
8.4. Parallel lines	31
9. Acknowledgement	32
References	32

## 1. INTRODUCTION

Let  $p$  be a prime number, and let  $k \in \mathbb{N}$ . We define  $R := \mathbb{Z}/p^k\mathbb{Z}$ , the ring of integers modulo  $p^k$ , and use  $R^\times$  to denote the multiplicative group of invertible elements of  $R$ . For  $x \in R^n$ , we write  $x = (x_1, \dots, x_n)$  in terms of coordinates. We also define the inner product on  $R^n$  as the  $R$ -valued function  $\langle x, y \rangle = x_1y_1 + \dots + x_ny_n$ .

Recall that the projective space  $\mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}$  is defined as the quotient space  $(\mathbb{Z}/p\mathbb{Z})^n / \sim$ , where  $\sim$  is the equivalence relation

$$b \sim b' \iff b = \lambda b' \text{ for some } \lambda \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}.$$

When  $k > 1$ , the projective space over  $R^n$  must be defined a little bit more carefully. Define the  $(n-1)$ -dimensional sphere  $\mathbb{S}^{n-1}(R)$  to be the set of all elements of  $R$  that have at least one invertible component. In particular,  $\mathbb{S}^0(R) = R^\times$ . We then define

$$\mathbb{P}R^{n-1} = \mathbb{S}^{n-1}(R) / \mathbb{S}^0(R).$$

We will refer to the elements of  $\mathbb{P}R^{n-1}$  as *nondegenerate directions* in  $R^n$ . Thus, two elements  $b, b'$  of  $\mathbb{S}^{n-1}(R)$  define the same direction if and only if

$$(1.1) \quad b = \lambda b' \text{ for some } \lambda \in R^\times.$$

This is how directions in  $R^n$  are often defined in the literature, see e.g. [12]. All directions will be assumed to be nondegenerate unless explicitly stated otherwise.

A *hyperplane* is a set of the form

$$H_b(a) = \{a \in R^n : \langle x - a, b \rangle = 0\},$$

for some  $a \in R^n$  and a nondegenerate direction  $b \in \mathbb{P}R^{n-1}$ . (Note that the equality  $\langle x - a, b \rangle = 0$  should hold in  $R$  and not just modulo  $p$ .) When  $a = 0$ , we write  $H_b = H_b(0)$ . We will sometimes refer to  $H_b$  as *homogeneous hyperplanes*, and to  $H_b(a)$  as *affine hyperplanes*. We also define

$$\mathcal{H}^n = \text{span}_{\mathbb{Z}/p\mathbb{Z}}\{\mathbf{1}_{H_b(a)} : a \in R^n, b \in \mathbb{P}R^{n-1}\},$$

considered as a set of functions from  $R^n$  to  $\mathbb{Z}/p\mathbb{Z}$ .

**Definition 1.1.** Let  $R = \mathbb{Z}/p^k\mathbb{Z}$ , where  $p$  is a prime and  $k \in \mathbb{N}$ .

- (i) The point-hyperplane incidence matrix of  $R^n$  is the matrix  $W_{p^k, n}$ , with rows and columns indexed by  $x \in R^n$ , such that

$$(W_{p^k, n})_{x, y} = \begin{cases} 1 & \text{if } \langle x, y \rangle = 0, \\ 0 & \text{otherwise.} \end{cases}$$

- (ii) The reduced point-affine hyperplane incidence matrix of  $R^n$  is the matrix  $\mathcal{A}_{p^k, n}^*$ , with rows indexed by  $(x, a) \in R^n \times R^n$  and columns indexed by  $b \in \mathbb{P}R^{n-1}$ , such that

$$(\mathcal{A}_{p^k, n}^*)_{(x, a), b} = \begin{cases} 1 & \text{if } x \in H_b(a), \\ 0 & \text{otherwise.} \end{cases}$$

- (iii) The reduced point-hyperplane incidence matrix of  $R^n$  is the matrix  $W_{p^k, n}^*$  with rows indexed by  $b \in \mathbb{P}R^{n-1}$  and columns indexed by  $x \in R^n$ , such that

$$(W_{p^k, n}^*)_{x, b} = \begin{cases} 1 & \text{if } x \in H_b, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the equation  $\langle x, y \rangle = 0$  in (i) does not define a hyperplane in our sense if  $y$  is not a direction; however, we use the terminology above for consistency with the existing literature such as [6].

We are interested in upper and lower bounds on the rank of these matrices over  $\mathbb{Z}/p\mathbb{Z}$ . For  $k = 1$ , the rank of  $W_{p,n}$  is known as a special case of the results in [11], [14], [16].

**Theorem 1.2** ([11], [14], [16]). *For  $p$  prime and  $n \in \mathbb{N}$ ,*

$$\text{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p,n}) = \binom{p+n-2}{n-1} + 1.$$

Theorem 1.2 can be deduced from a characterization of hyperplane functions in  $\mathbb{F}_p^n$  in terms of polynomials. Specifically, when  $k = 1$ ,  $\mathcal{H}^n$  is identical to  $\mathbb{F}_p[x_1, \dots, x_n]$ , the space of all polynomials in  $n$  variables of total degree at most  $p - 1$  over  $\mathbb{F}_p$ . Moreover, the subspace  $\mathcal{H}_0^n$  spanned by homogeneous hyperplanes is identical to the linear span of all homogeneous polynomials in  $\mathbb{F}_p[x_1, \dots, x_n]$  of degree exactly  $p - 1$ , together with the constant function. Counting all such polynomials produces the bound in Theorem 1.2. We provide the full argument in Section 5.2.

For  $k \geq 2$ , this method is no longer feasible. By Fermat's Little Theorem, a polynomial over  $R$  can have degree at most  $p - 1$  in each variable, hence there are not sufficiently many polynomials to span all hyperplane functions. We remedy this by using binomial coefficients as generalized polynomial functions. This allows us to define generalized polynomials of degree up to  $p^k - 1$ , which is sufficient to span  $\mathcal{H}^n$ . Binomial coefficients were used in lieu of polynomials in [2] for the purpose of extending the Ellenberg-Gijswijt bound on cap sets [10] to  $R^n$ ; see also [15] for an argument based on a more abstract concept of generalized polynomials, and [17] for a third approach to cap sets in  $R^n$  and a discussion of the relationship between these methods. We are not aware, however, of any previous applications of similar methods to studying hyperplane functions.

In Proposition 5.9, we prove that hyperplane functions in  $R^n$  are, in this sense, generalized  $n$ -variate polynomials of degree up to  $p^k - 1$ . This implies our first theorem.

**Theorem 1.3.** *For  $p$  prime and  $k, n \in \mathbb{N}$ , we have*

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{H}^n) = \text{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}_{p^k,n}^*) \leq \binom{p^k - 1 + n}{n}.$$

However, unlike for  $k = 1$ , hyperplane functions in  $R^n$  with  $k \geq 2$  need not span all such generalized polynomials. In fact, we have the following bound, which is strictly lower than that in Theorem 1.3 when  $k \geq 2$  and  $n$  is small relative to  $p^k$ .

**Theorem 1.4.** *Let  $p$  be prime, and let  $k, n \in \mathbb{N}$ . Then*

$$(1.2) \quad \text{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}_{p^k,n}^*) \leq (2n) \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n},$$

Theorems 1.3 and 1.4 imply upper bounds on the ranks of  $W_{p^k,n}^*$  and  $W_{p^k,n}$ , via the next proposition.

**Proposition 1.5.** *Let  $n \in \mathbb{N}$ ,  $n \geq 2$ . Then*

$$\text{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n}) \leq 1 + k \cdot \text{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n}^*),$$

$$\text{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k, n+1}^*) \leq 2(k+1) \cdot \text{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}_{p^k, n}^*).$$

Theorem 1.4 raises the question of how we can tell whether a given generalized polynomial of degree at most  $p^k - 1$  is a hyperplane function. Our generalized polynomials share many geometric properties of hyperplane functions. For example, if  $L, L'$  are two parallel lines in  $R^n$ , then  $|L \cap H| \equiv |L' \cap H| \pmod{p}$  for any hyperplane  $H$ ; we prove in Proposition 8.12 that an appropriate analogue of this holds for generalized polynomials of degree up to  $p^k - 1$ . Nonetheless, we are able to find a class of functions on  $R^n$  we call *fans* that are orthogonal over  $\mathbb{Z}/p\mathbb{Z}$  to all hyperplane functions, but not to some of our generalized polynomials of degree up to  $p^k - 1$ . Essentially, this test identifies generalized polynomials that behave like hyperplane functions on each scale separately, but the directions are not consistent between the scales. Since the statement of the result requires some notation, we postpone it to Section 8. While a generalized polynomial must satisfy our orthogonality condition in order to be a hyperplane function, we do not know whether this condition is also sufficient.

Our interest in hyperplane functions is motivated in part by the recent work of Dhar and Dvir [6], where a connection was established a connection between point-hyperplane incidence matrices and the Kakeya problem. For  $k = 1$ , Dhar and Dvir used Theorem 1.2 to give a new proof of Dvir's result [7] that a Kakeya set  $S \subset (\mathbb{Z}/p\mathbb{Z})^n$  must satisfy  $|S| \gtrsim_{\epsilon} p^{n-\epsilon}$  for any  $\epsilon > 0$ . They were then able to extend this matrix-based argument to prove the Kakeya conjecture in  $\mathbb{Z}/N\mathbb{Z}$  for squarefree  $N$ . In  $R = \mathbb{Z}/p^k\mathbb{Z}$  with  $k \geq 2$ , Dhar and Dvir were still able to bound the size of Kakeya sets in  $R^n$  from below by the  $\mathbb{F}_p$ -rank of  $W_{p^k, n}^*$ . (In [6, Theorem 1.6], the authors refer to the rank of  $W_{p^k, n}$ ; however, their argument uses the matrix  $W_{p^k, n}^*$  instead. The two ranks are not equal, but they are comparable; see Lemma 2.1 and Proposition 2.2.)

Unfortunately, relatively little has been known about the  $\mathbb{F}_p$ -rank of point-hyperplane incidence matrices in  $R^n$ . Dhar and Dvir [6, Lemma 5.3] observe that the rank of  $W_{p^k, n}$  is bounded from below by the size of a maximal *matching vector family* in  $R^n$ . Combining this with the results of [8, 18] yields a lower bound on the rank of  $W_{p^k, n}$  of the order  $p^{kn/2}$ , therefore a lower bound of the same order on the size of Kakeya sets in  $R^n$ . Dhar and Dvir observe further that, in light of an upper bound on the size of matching vector families given in [9], this method cannot yield significantly better lower bounds.

The Kakeya conjecture in  $R^n$  was eventually resolved by Arsovski [1], based on a comparison of the size of Kakeya sets to the rank of a different matrix that, in general, may have higher rank than  $W_{p^k, n}$ . Subsequently, Dhar [3] proved the Kakeya conjecture in  $\mathbb{Z}/N\mathbb{Z}$  for general  $N$ , with further progress in [4, 5].

The question of the rank of the point-hyperplane incidence matrices in Definition 1.1 was left open. While this is no longer needed for the Kakeya problem, we believe it to be of independent interest, as it provides a good testing ground for variants of the polynomial method that rely on generalized polynomials.

This paper is organized as follows. We study the relationships between the ranks of the different incidence matrices in Section 2. Proposition 1.5 follows from Propositions 2.2 and 2.3. In Section 3, we define our generalized polynomials in one variable based on binomial coefficients. The rest of Section 3, as well as Section 4, are dedicated to the study of the properties of these functions. An important feature of a “generalized polynomial” of degree

$m$  is that its derivatives of order  $m + 1$  should vanish; we prove in Lemma 4.4 that our binomial functions have this property.

In Section 5, we extend our generalized polynomials to  $R^n$  and prove that they are, again, well behaved with respect to discrete derivatives. We also prove that hyperplane functions in  $R^n$  are generalized polynomials of degree at most  $p^k - 1$ . In particular, Theorem 1.3 follows from Proposition 5.9. We note that, while an *ad hoc* application of binomial coefficients was sufficient in [2], we need to develop our theory more systematically.

A major difficulty in working with binomial coefficients is that they do not have good multiplicative properties. This is one reason why there is no straightforward way to adapt the methods from the  $k = 1$  case to our setting (and why, for the time being, we are only able to prove partial results). This turns out to be more than just a technical issue. Our results in Section 6 show that the behaviour of our generalized polynomials is genuinely different than that of classical polynomials. For example,  $(xy)^m = x^m y^m$  is a bivariate polynomial of degree  $2m$ ; on the other hand, if  $f$  is a generalized polynomial of degree  $m$  on  $R$ , then the degree of  $f(xy)$  cannot be much larger than  $m$ . This degree reduction is the main idea behind the proof of Theorem 1.4 in Section 7.

Finally, in Section 8 we study the geometric properties of lines and hyperplanes in  $R^n$ , and develop a test that (at least in some cases) allows us to determine that a given generalized polynomial is not a hyperplane function.

Throughout this article, we will observe the following conventions. Arithmetic operations and equalities for elements of  $R$  will be defined in  $R$ , that is, modulo  $p^k$ . For example, if  $a, b \in R$ , the equality  $a = b$  will mean that  $a \equiv b \pmod{p^k}$ . When we work with functions with values in  $\mathbb{Z}/p\mathbb{Z}$  (such as the  $\phi_m$  functions defined in (3.1)), all arithmetic operations and equalities involving such functions will be understood to hold in  $\mathbb{Z}/p\mathbb{Z}$ . In expressions such as  $af(x)$ , where  $a, x \in R$  and  $f$  is a function  $R \rightarrow \mathbb{Z}/p\mathbb{Z}$ , we will interpret  $a$  as the function  $a \rightarrow (a \bmod p)$ , so that  $af(x)$  refers to the function  $(a \bmod p)f(x)$  with values in  $\mathbb{Z}/p\mathbb{Z}$ . The inner product in  $R$  is an  $R$ -valued function, so that  $\langle x, y \rangle = c$  means that  $x_1 y_1 + \cdots + x_n y_n \equiv c \pmod{p^k}$  and not just mod  $p$ . On the other hand, if  $f, g$  are two functions from  $R^n$  to  $\mathbb{Z}/p\mathbb{Z}$ , their inner product

$$\langle f, g \rangle = \sum_{x \in R^n} f(x)g(x)$$

takes values in  $\mathbb{Z}/p\mathbb{Z}$ .

In line with our use of functions with range in  $\mathbb{Z}/p\mathbb{Z}$ , whenever we refer to the rank of a matrix, the span of a set of vectors, or the dimension of a linear space of functions, this rank, span, or dimension is taken over  $\mathbb{Z}/p\mathbb{Z}$  unless explicitly stated otherwise.

For  $m \in \mathbb{N}$ , we write  $[m] = \{0, 1, \dots, m - 1\} \subset \mathbb{Z}$ . We will distinguish between  $R$ , a ring with addition and multiplication mod  $p^k$ , and  $[p^k]$ , a set of integers where addition and multiplication are inherited from  $\mathbb{Z}$  (so that  $[p^k]$  is not closed under these operations). Exponents, indices, etc. will always be integers unless stated explicitly otherwise. For example, if  $\ell$  is the degree of a polynomial or a generalized polynomial, we will write  $\ell \in [p^k]$  and not  $\ell \in R$ .

We use the notation  $|S|$  to denote the cardinality of a set  $S$ , and the notation  $p^j \parallel a$  to mean  $p^j \mid a$  but  $p^{j+1} \nmid a$ . We also use subscripts  $1, \dots, n$  to denote both the coordinates  $x = (x_1, \dots, x_n)$  of a point  $x \in R^n$  and the  $p$ -adic digits in the expansion  $x = \sum_{j=0}^{k-1} x_j p^j$  of

an element  $x \in R$ . This should not cause confusion, since we will only use one of the above at a time and the meaning will be clear from context. Whenever we mention the  $p$ -adic expansion or  $p$ -adic digit of a number  $x$ , we refer to the unique expansion  $x = \sum_{j=0}^k x_j p^j$  with  $x_j \in \{0, 1, \dots, p-1\}$  for all  $j$ .

## 2. RELATIONSHIPS BETWEEN INCIDENCE MATRICES

We first observe that

$$(2.1) \quad \text{rank}(W_{p^k, n}^*) \leq \text{rank}(W_{p^k, n}),$$

since the rows of  $W_{p^k, n}^*$  form a subset of the rows of  $W_{p^k, n}$ . Lemma 2.1 shows that the inequality can be strict for  $k \geq 2$ .

**Lemma 2.1.** *If  $k \in \mathbb{N}$  and  $k \geq 2$ , then  $\text{rank}(W_{p^k, 2}) > \text{rank}(W_{p^k, 2}^*)$ .*

*Proof.* All directions in  $R^2$  can be represented by one of the elements of the set

$$\mathcal{D} = \{(1, i) : i \in R\} \cup \{(jp, 1) : j \in \{0, 1, \dots, p^{k-1} - 1\}\}.$$

Given a direction  $b \in R^2$ , define

$$L_b = \{tb : t \in R\}.$$

Given  $b \in \mathcal{D}$ , there is some  $c \in \mathcal{D}$  such that  $H_b = \text{span}(c) := \{\lambda c : \lambda \in R\}$ . Let

$$\mathcal{H} = \{\mathbf{1}_{H_b} : b \in \mathcal{D}\} = \{\mathbf{1}_{L_b} : b \in \mathcal{D}\}.$$

Then  $\mathcal{H}$  consists of exactly the rows of  $W_{p^k, 2}^*$ , and is a subset of the rows of  $W_{p^k, 2}$ .

Let  $y = (p^{k-1}, 0)$ , then the indicator function of  $H_y := \{x \in R^n : \langle x, y \rangle = 0\}$  is a row of  $W_{p^k, 2}$ . We claim that

$$\mathbf{1}_{H_y} \notin \text{span} \mathcal{H}.$$

Assume towards contradiction that there are scalars  $\alpha_i, \beta_j$  such that

$$(2.2) \quad \mathbf{1}_{H_y}(x) = \sum_{i=0}^{p^k-1} \alpha_i \mathbf{1}_{L_{(1,i)}}(x) + \sum_{j=0}^{p^{k-1}-1} \beta_j \mathbf{1}_{L_{(pj,1)}}(x).$$

We first evaluate (2.2) at  $x = (pj, 1)$  for  $j \in \{0, \dots, p^{k-1} - 1\}$ . Since  $(pj, 1) \in H_y$  but

$$(pj, 1) \notin L_{(1,i)}, \quad (pj, 1) \notin L_{(p\ell, 1)} \text{ if } j \neq \ell,$$

it follows that  $\beta_j = 1$  for all  $j$ . Now evaluate (2.2) at  $x = (0, p^{k-1})$ . Since

$$(0, p^{k-1}) \notin L_{(1,i)} \text{ for all } i, \text{ but } (0, p^{k-1}) \in L_{(pj, 1)} \text{ for all } j,$$

we have

$$\sum_{i=0}^{p^k-1} \alpha_i \mathbf{1}_{L_{(1,i)}}(0, p^{k-1}) + \sum_{j=0}^{p^{k-1}-1} \beta_j \mathbf{1}_{L_{(pj,1)}}(0, p^{k-1}) = p^{k-1} = 0 \pmod{p}.$$

This is a contradiction, as  $(0, p^{k-1}) \in H_y$ . □

In the next proposition, we provide a partial converse to the inequality in (2.1).

**Proposition 2.2.** *Let  $n \geq 2$  and  $k \geq 1$ . Then*

$$\text{rank}(W_{p^k,n}) \leq 1 + \sum_{j=1}^k \text{rank}(W_{p^j,n}^*),$$

and consequently,

$$\text{rank}(W_{p^k,n}) \leq 1 + k \cdot \text{rank}(W_{p^k,n}^*).$$

*Proof.* Recall that the columns of  $W_{p^k,n}$  are indexed by  $b \in R^n$ . Partition these columns by the sets

$$B_j = \{b' \in R^n : b' = p^j b, b \neq 0 \pmod{p}\},$$

and let  $W^{(j)}$  be the submatrix of  $W_{p^k,n}$  consisting of columns indexed by  $b' \in B_j$ . Then

$$\text{rank}(W_{p^k,n}) \leq \sum_{j=0}^k \text{rank}(W^{(j)}).$$

Note that the only vector in  $B_k$  is the zero vector, and so  $W^{(0)}$  is just a column of all 1s, which has rank 1. Thus to prove the proposition, it suffices to show that for  $j \in [k]$ , we have  $\text{rank}(W^{(j)}) \leq \text{rank}(W_{p^{k-j},n})$ . We show that this actually holds with equality.

Let  $j \in [k]$ . The column of  $W^{(j)}$  corresponding to  $b' \in B_j$  is the indicator vector of  $\{x \in R^n : \langle x, b' \rangle = 0 \pmod{p^k}\}$ . Recalling that  $b' = p^j b$  for a direction  $b$ , we have

$$(2.3) \quad \langle x, b' \rangle = 0 \pmod{p^k} \quad \text{if and only if} \quad \langle x, b \rangle = 0 \pmod{p^{k-j}}.$$

Notice that the latter equation only depends on  $x \pmod{p^{k-j}}$ ; we will use this observation to partition the rows of  $W^{(j)}$ .

For  $\ell \in [k]$ , let  $\overline{R}_\ell^n$  be the set of  $x \in R^n$  so that for each  $i \geq \ell$ , the  $i$ -th  $p$ -adic digit of each component of  $x$  is zero. Consider the sets

$$X_u := up^{k-j} + \overline{R}_{k-j}^n, \quad u \in \overline{R}_j^n.$$

Let  $W_u^{(j)}$  be the submatrix of  $W^{(j)}$  consisting of rows indexed by  $x \in X_u$ . By definition, for each  $u$ , the set  $\{x \pmod{p^{k-j}} : x \in X_u\}$  can be identified with  $R_{k-j}^n$ . Similarly, the set  $\{b : p^j b \in B_j\}$  can be identified with the set of directions of  $R_{k-j}^n$ . Combining these observations with the equivalence in (2.3), we see that  $W_u^{(j)}$  is the same matrix as  $W_{p^{k-j},n}^*$ . As this is true for each  $u$ , the matrix  $W^{(j)}$  is formed by vertically concatenating copies of  $W_{p^{k-j},n}^*$ . Thus it has the same rank as  $W_{p^{k-j},n}^*$ , as claimed.  $\square$

**Proposition 2.3.** *Let  $n \in \mathbb{N}$ ,  $n \geq 2$ . Then*

$$(2.4) \quad \text{rank}(\mathcal{A}_{p^k,n}^*) \leq \text{rank}(W_{p^k,n+1}^*) \leq 2(k+1) \cdot \text{rank}(\mathcal{A}_{p^k,n}^*).$$

*Proof.* We write directions  $b \in R^{n+1}$  as  $b = (\tilde{b}, b_{n+1})$ , with  $\tilde{b} \in R^n$ . By a mild abuse of notation, we identify  $b$  with an element of  $\mathbb{P}R^n$ . We use a similar convention for points  $x \in R^{n+1}$ .

We first prove that  $\text{rank}(\mathcal{A}_{p^k,n}^*) \leq \text{rank}(W_{p^k,n+1}^*)$ . Any affine hyperplane in  $R^n$  can be written as

$$(2.5) \quad \tilde{H}_b = \left\{ \tilde{x} \in R^n : \langle \tilde{x}, \tilde{b} \rangle = -b_{n+1} \right\},$$

where  $\tilde{b} \in \mathbb{P}R^{n-1}$  is a direction, and  $b_{n+1} \in R$ . For any such  $(\tilde{b}, b_{n+1})$ , let

$$(2.6) \quad H_b = \left\{ x = (\tilde{x}, x_{n+1}) \in R^{n+1} : \langle \tilde{x}, \tilde{b} \rangle + b_{n+1}x_{n+1} = 0 \right\},$$

so that  $\tilde{H}_b \times \{1\} = H_b \cap \{x \in R^{n+1} : x_{n+1} = 1\}$ . Consider the submatrix of  $W_{p^k, n+1}^*$  obtained by restricting to rows indexed by  $(\tilde{b}, b_{n+1}) \in \mathcal{B} := \mathbb{P}R^{n-1} \times R$  and columns indexed by  $x \in R^n \times \{1\}$ . By the above correspondence, this submatrix is a copy of  $\mathcal{A}_{p^k, n}^*$ , giving the desired bound.

When considering the converse of this argument, it might be possible for a set of columns of the submatrix defined above to be linearly dependent even if the corresponding columns of the larger matrix  $W_{p^k, n}^*$  are linearly independent. We remedy this by considering linear independence on each scale separately.

For  $j \in \{0, 1, \dots, k\}$ , let  $X_j = \{x \in R^{n+1} : x_{n+1} = p^j y, y \neq 0 \pmod{p}\}$ . Let  $W^{(j)}$  be the submatrix of  $W_{p^k, n+1}^*$  formed by restricting to the columns with  $x \in X_j$ . Then

$$\text{rank}(W_{p^k, n+1}^*) \leq \sum_{j=0}^k \text{rank}(W^{(j)}).$$

We will show that  $\text{rank}(W^{(j)}) \leq 2 \cdot \text{rank}(\mathcal{A}_{p^k, n}^*)$  for each  $j \in \{0, 1, \dots, k\}$ , implying the second bound in (2.4).

Let  $W_1^{(j)}$  be the submatrix formed by restricting to the rows indexed by  $b \in \mathcal{B}$ , and let  $W_2^{(j)}$  be the submatrix consisting of the remaining rows. Clearly,  $\text{rank}(W^{(j)}) \leq \text{rank}(W_1^{(j)}) + \text{rank}(W_2^{(j)})$ . It therefore suffices to prove that

$$(2.7) \quad \text{rank}(W_i^{(j)}) \leq \text{rank}(\mathcal{A}_{p^k, n}^*) \text{ for } i = 1, 2.$$

We first prove (2.7) for  $i = 1$ . For each  $b = (\tilde{b}, b_{n+1}) \in \mathcal{B}$ , let  $H_b = \{x \in R^{n+1} : \langle x, b \rangle = 0\}$ , and let

$$\tilde{H}_{b,j} = \{\tilde{x} \in R^n : \langle \tilde{x}, \tilde{b} \rangle = -p^j b_{n+1}\},$$

so that  $\tilde{H}_{b,j} \times \{p^j\} = H_b \cap \{x \in R^{n+1} : x_{n+1} = p^j\}$ . We first note that

$$(2.8) \quad \text{rank}(W_1^{(j)}) \leq \dim(\text{span}\{\mathbf{1}_{H_b \cap X_j} : b \in \mathcal{B}_j\}),$$

where  $\mathcal{B}_j = \{b \in \mathcal{B} : b_{n+1} \in [p^{k-j}]\}$ . This is because, for  $x \in X_j$ , the value of  $\mathbf{1}_{H_b}(x)$  is determined uniquely by  $\tilde{b}$  and the first  $k-j$  digits in the  $p$ -adic expansion of  $b_{n+1}$ . Next, we prove that

$$(2.9) \quad \dim(\text{span}\{\mathbf{1}_{H_b \cap X_j} : b \in \mathcal{B}_j\}) \leq \dim(\text{span}\{\mathbf{1}_{\tilde{H}_{b,j}} : b \in \mathcal{B}_j\}).$$

For  $j = k$ , we have  $X_k = \{(\tilde{x}, 0) : \tilde{x} \in R^n\}$  and  $\mathcal{B}_k = \{(\tilde{b}, 0) : \tilde{b} \in R^n\}$ , so that for  $b \in \mathcal{B}_k$  we have  $H_b \cap X_k = \tilde{H}_{b,k} \times \{0\}$  and the claim is clear.

We now assume that  $j \leq k-1$ . Suppose that there are scalars  $c_b$  so that

$$(2.10) \quad \sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{\tilde{H}_{b,j}} = 0.$$



We will show that  $\sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{H_b \cap X_j} = 0$  as well. For  $s \in [p^{k-j}]$ ,  $s \neq 0 \pmod p$ , define

$$X_{j,s} = \{x \in X_j : x_{n+1} = sp^j\}.$$

First, we note that as  $s$  is invertible,

$$(2.11) \quad H_b \cap X_{j,s} = \{(s\tilde{x}, sp^j) : \tilde{x} \in \tilde{H}_{b,j}\}$$

and as the  $X_{j,s}$  form a partition for  $X_j$ ,

$$\mathbf{1}_{H_b \cap X_j} = \sum_s \mathbf{1}_{H_b \cap X_{j,s}}.$$

Then

$$\sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{H_b \cap X_j} = \sum_{b \in \mathcal{B}_j} c_b \sum_s \mathbf{1}_{H_b \cap X_{j,s}} = \sum_s \left( \sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{H_b \cap X_{j,s}} \right)$$

But each term in the outermost sum of the right-hand side of this equation is equal to zero, by (2.11) and (2.10). Thus  $\sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{H_b \cap X_j} = 0$ , proving (2.9).

Combining (2.8) and (2.9), we get

$$\text{rank}(W_1^{(j)}) \leq \dim \left( \text{span} \{ \mathbf{1}_{\tilde{H}_{b,j}}(b) : b \in B_j \} \right) \leq \text{rank}(\mathcal{A}_{p^k,n}^*).$$

as claimed.

To prove (2.7) for  $i = 2$ , we observe that if  $b = (\tilde{b}, b_{n+1}) \notin \mathcal{B}$ , then  $\tilde{b}$  is not a direction in  $R^n$ , hence none of  $b_1, \dots, b_n$  are invertible. Since  $b$  is a direction in  $R^{n+1}$ , we have  $b_{n+1} \in R^\times$ , so that  $b = (b_1, \tilde{b})$  for a direction  $\tilde{b} \in R^n$ . The desired bound follows by the same argument as above with the first and last coordinates interchanged.  $\square$

### 3. THE BINOMIAL PHI FUNCTIONS

**3.1. Definitions.** In this section, we work in  $R = \mathbb{Z}/p^k\mathbb{Z}$  and use the representatives  $R = \{0, 1, 2, \dots, p^k - 1\}$ . Given two elements  $x, y \in R$ , we will write that  $x < y$ ,  $x \leq y$ , etc. if the stated inequality holds for the representatives of  $x, y$  chosen above.

**Definition 3.1.** For  $m \in [p^k]$ , we define the functions  $\phi_m : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  by

$$(3.1) \quad \phi_m(x) = \binom{x}{m} \pmod p,$$

with the convention that  $\binom{0}{0} = 1$  and  $\binom{a}{b} = 0$  for  $a < b$ . We also define for all  $x \in R$ ,

$$(3.2) \quad \phi_m(x) = 0 \text{ if } m < 0 \text{ or } m \geq p^k.$$

The binomial coefficients above are well defined by Lucas's Theorem, which we recall here for the reader's convenience.

**Theorem 3.2 (Lucas's Theorem).** Let  $p$  be prime. Let  $m, n$  be nonnegative integers with  $p$ -adic expansions  $m = \sum_{j=0}^{\ell} m_j p^j$  and  $n = \sum_{j=0}^{\ell} n_j p^j$ , where  $m_j, n_j \in [p]$ . Then, with the same convention as above,

$$\binom{m}{n} \equiv \prod_{j=0}^{\ell} \binom{m_j}{n_j} \pmod p.$$

**Proposition 3.3.** *If  $x, y \in \mathbb{Z}_{\geq 0}$  satisfy  $x \equiv y \pmod{p^k}$ , then  $\binom{x}{m} \equiv \binom{y}{m} \pmod{p}$ . Consequently,  $\phi_m$  are well-defined as functions on  $R$ . They satisfy the recurrence relations*

$$(3.3) \quad \begin{aligned} \phi_0(x) &= 1 \text{ for all } x \in R, & \phi_m(0) &= 0 \text{ for all } m \neq 0, \\ \phi_m(x+1) &= \phi_m(x) + \phi_{m-1}(x) \text{ for } m \in [p^k]. \end{aligned}$$

Furthermore, if  $m \in [p^k]$  and  $x \in R$  have the  $p$ -adic expansions  $m = \sum m_i p^i$  and  $x = \sum x_i p^i$ , then

$$(3.4) \quad \phi_m(x) = \prod_{i=0}^{k-1} \phi_{m_i}(x_i).$$

*Proof.* The first conclusion is trivial when  $m < 0$  or  $m \geq p^k$ , since then  $\phi_m(x) = 0$  for all  $x$ . Assume now that  $m \in [p^k]$  and that  $x \equiv y \pmod{p^k}$  for some  $x, y \in \mathbb{Z}_{\geq 0}$ . Then the  $p$ -adic expansions  $x = \sum x_j p^j$  and  $y = \sum y_j p^j$  satisfy  $x_j = y_j$  for  $0 \leq j \leq k-1$ , and the conclusion follows from Lucas's Theorem.

Part (3.3) follows directly from (3.1), (3.2), and Pascal's identity for binomial coefficients. Finally, (3.4) is Lucas's Theorem again.  $\square$

We will view the functions  $\phi_m$  as “generalized polynomials” on  $R$ . For  $m = 0, 1, \dots, p-1$ , we will see that  $\phi_m$  is in fact a polynomial of degree  $m$  (Corollary 5.7 with  $n = 1$ ). We have  $\phi_0(x) = 1$  and  $\phi_1(x) = x$  for all  $x$ , but  $\phi_m$  with  $2 \leq m < p$  need not be either homogeneous or monic. For  $m \geq p$ , (3.1) still makes sense and defines additional functions that can be thought of as “polynomial” of degree  $m$ , for example in the sense of [13].

Unlike for actual polynomials, there is no canonical choice of homogeneous generalized polynomials on  $R^n$ . For example, we could have defined  $\phi_m(x) := \binom{x+m}{m}$  instead of (3.1), and all our proofs would have been essentially the same with only slightly more complicated calculations. We further note that the recurrence relation (3.3) could be used as an alternative (but equivalent) definition of phi functions.

For  $k = 1$ , the polynomials  $1, x, x^2, \dots, x^{p-1}$  are linearly independent functions on  $\mathbb{Z}/p\mathbb{Z}$ , therefore form a linear basis for the space of all functions on  $\mathbb{Z}/p\mathbb{Z}$ . We now prove that the same is true for the functions  $\phi_m$  for general  $k$ .

**Lemma 3.4. (Linear independence of  $\phi_m$ )** *Let  $\Phi$  be the  $p^k \times p^k$  matrix with columns indexed by  $x \in R$  and rows by  $m \in [p^k]$ , and with entries*

$$\Phi_{m,x} = \phi_m(x).$$

*Then  $\Phi$  is a nonsingular upper triangular matrix, with  $\Phi_{m,m} = \binom{m}{m} = 1$  and  $\Phi_{m,x} = 0$  for  $x < m$ . Consequently, the functions  $\{\phi_m\}_{m \in [p^k]}$  are linearly independent over  $\mathbb{Z}/p\mathbb{Z}$ , and form a basis for the space of all functions from  $R$  to  $\mathbb{Z}/p\mathbb{Z}$ .*

*Proof.* We clearly have  $\Phi_{m,m} = \binom{m}{m} = 1$  for all  $m \in [p^k]$ . If  $x, m \in [p^k]$  with  $x < m$ , then at least one  $p$ -adic digit of  $x$  must be smaller than the corresponding  $p$ -adic digit of  $m$ , so that  $\binom{x}{m} = 0$  by Lucas's Theorem. It follows that  $\Phi$  is an upper triangular matrix, nonsingular since all its diagonal entries are equal to 1. Since the  $m$ -th row of  $\Phi$  is the list of values of  $\phi_m(x)$  as  $x \in R$ , the linear independence of the rows of  $\Phi$  implies the linear independence of  $\phi_m$  with  $m \in [p^k]$ . In particular, the linear span of  $\{\phi_m\}_{m \in [p^k]}$  over  $\mathbb{Z}/p\mathbb{Z}$  has dimension  $p^k$ .

Since this is also the dimension of the the space of all functions from  $R$  to  $\mathbb{Z}/p\mathbb{Z}$ , the last statement follows.  $\square$

**3.2. Properties of phi functions.** Vandermonde's Identity (3.5) is the phi-function analogue of the binomial expansion of  $(x + y)^m$ . Unfortunately, the simple polynomial formula  $(xy)^m = x^m y^m$  has a far less transparent analogue (3.6) for phi functions. A significant amount of work in the sequel will go towards studying the multiplicative properties of  $\phi_m$ .

**Lemma 3.5.** (*Vandermonde's Identity*) For  $m \in [p^k]$  and  $x, y, b \in R$ , we have

$$(3.5) \quad \phi_m(x + y) = \sum_{i=0}^m \phi_i(x) \phi_{m-i}(y),$$

$$(3.6) \quad \phi_m(bx) = \sum_{i_1 + \dots + i_b = m} \phi_{i_1}(x) \dots \phi_{i_b}(x).$$

*Proof.* Equation (3.5) is known in the literature, but we include the short proof for completeness. For  $m = 0$ , the only pair  $i, j$  with  $i + j = m$  is  $i = j = 0$ , and  $\phi_0(x + y) = 1 = \phi_0(x) \phi_0(y)$ . For  $m = 1, \dots, p^k - 1$ , we prove (3.5) by induction in  $y$ . The formula is clearly true for  $y = 0$ , since then the only nonzero term on the right side of (3.5) is  $\phi_m(x) \phi_0(0) = 1$ . Assume now that (3.5) holds for some  $y \in R$  and all  $x \in R$ . Then, by the inductive assumption, two applications of (3.3), and the convention that  $\phi_{-1} = 0$ :

$$\begin{aligned} \phi_m(x + (y + 1)) &= \phi_m((x + 1) + y) = \sum_{i=0}^m \phi_i(x + 1) \phi_{m-i}(y) \\ &= \sum_{i=0}^m (\phi_i(x) + \phi_{i-1}(x)) \phi_{m-i}(y) \\ &= \sum_{i=0}^m \phi_i(x) (\phi_{m-i-1}(y) + \phi_{m-i}(y)) \\ &= \sum_{i=0}^m \phi_i(x) \phi_{m-i}(y + 1) \end{aligned}$$

as claimed. The second identity (3.6) follows by iterating (3.5).  $\square$

**Lemma 3.6.** For  $m \in [p^{k-j}]$  and  $j \in \{1, \dots, k - 1\}$ , we have

$$(3.7) \quad \phi_{p^j m}(p^j x) = \phi_m(x).$$

Additionally,  $\phi_m(p^j x) = 0$  if  $p^j$  does not divide  $m$ .

*Proof.* This is an immediate consequence of (3.4).  $\square$

## 4. DISCRETE DERIVATIVES

**4.1. Definitions.** A generalized polynomial of degree  $m$  is expected to vanish after the successive application of  $m + 1$  derivatives. We prove in Lemma 4.4 that this is true for our phi functions. We start by defining the *degree* of a function.

**Definition 4.1.** For  $m \in [p^k]$ , define  $\Omega_m := \text{span}\{\phi_\ell : 0 \leq \ell \leq m\}$ . We say that

- $f$  has degree at most  $m$  if  $f \in \Omega_m$ ,
- $f$  has degree equal to  $m$  if  $f \in \Omega_m \setminus \Omega_{m-1}$ ,
- two functions  $f, g$  are equal up to degree  $\ell$  if  $f - g \in \Omega_\ell$ ; we write this as  $f =_\ell g$ .

For convenience, we set  $\Omega_m := \{0\}$  for  $m < 0$ , so that a function  $f$  has negative degree if and only if  $f$  is the zero function.

**Definition 4.2. (Discrete derivatives)** Let  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$ . We define:

$$(4.1) \quad \begin{aligned} \Delta_c f(x) &:= f(x+c) - f(x) \text{ for } c \in R, \\ D_c f(x) &:= c^{-1}(f(x+c) - f(x)) = c^{-1}\Delta_c f(x) \text{ for } c \in R^\times. \end{aligned}$$

As per our convention for functions with values in  $\mathbb{Z}/p\mathbb{Z}$ , the factor  $c^{-1}$  in (4.1) is taken to mean  $(c^{-1} \bmod p) \in \mathbb{Z}/p\mathbb{Z}$ . For short, we will also write

$$Df = D_1 f = \Delta_1 f.$$

It follows from (3.3) that

$$(4.2) \quad \forall m \in [p^k], \quad D\phi_m = \phi_{m-1}.$$

By Lemma 3.4, any function  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  has an expansion  $f = \sum c_j \phi_j$ . Applying (4.2), we get

$$(4.3) \quad \forall m \in [p^k], \quad f \in \Omega_m \Leftrightarrow Df \in \Omega_{m-1}.$$

**Lemma 4.3.** Let  $m \in [p^k]$  and  $c \in R$ . Then:

- (i)  $\Delta_c \phi_m - c\phi_{m-1} \in \Omega_{m-2}$ ,
- (ii) If  $c \in R^\times$ , then  $D_c \phi_m - \phi_{m-1} \in \Omega_{m-2}$ .

Consequently, if  $f \in \Omega_m$ , then  $\Delta_c f \in \Omega_{m-1}$  for all  $c \in R$ , and  $D_c f \in \Omega_{m-1}$  for all  $c \in R^\times$ .

*Proof.* If  $m = 0$ , then  $\Delta_c \phi_m = 0$  for all  $c \in R$  and the lemma is satisfied trivially. Assume now that  $m > 0$ . By (3.5), we have

$$\begin{aligned} \phi_m(x+c) - \phi_m(x) &= \sum_{\ell=0}^m \phi_{m-\ell}(c)\phi_\ell(x) - \phi_m(x) \\ &= c\phi_{m-1}(x) + \sum_{\ell=0}^{m-2} \phi_{m-\ell}(c)\phi_\ell(x), \end{aligned}$$

where we used that  $\phi_0(c) = 1$  and  $\phi_1(c) = c$ . This implies the lemma.  $\square$

**Lemma 4.4.** For  $m \in [p^k]$  and  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$ , the following are equivalent:

- (i)  $f \in \Omega_{m-1}$ ,
- (ii)  $D^m f = 0$ ,
- (iii) For any choice of  $c_1, \dots, c_m \in R$  we have  $\Delta_{c_m} \dots \Delta_{c_1} f = 0$ .

*Proof.* The implication (i)  $\Rightarrow$  (iii) follows by iterating Lemma 4.3  $m$  times and using that  $\Omega_{-1} = \{0\}$ . Clearly (iii) implies (ii), by letting  $c_1 = \dots = c_m = 1$ .

To prove that (ii) implies (i), we argue by contrapositive. Assume that  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  has degree exceeding  $m - 1$ . Then there is some  $\ell \geq m$ , a non-zero constant  $c$ , and some function  $g$  of degree at most  $\ell - 1$  so that  $f = c\phi_\ell + g$ . By (4.2), we have

$$D^m f = c\phi_{\ell-m} + D^m g.$$

Since  $D^m g \in \Omega_{\ell-1-m}$  and  $c \neq 0$ , it follows from linear independence of the phi functions that  $D^m f$  is not the zero function.  $\square$

## 4.2. More properties of phi functions.

**Lemma 4.5.** *Let  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  be a function, and let  $x = \sum_{j=0}^{k-1} x_j p^j$  be the  $p$ -adic expansion of the variable  $x \in R$ . Let  $\ell \in \{0, 1, \dots, k-1\}$ . Then:*

(i)  $f \in \Omega_{p^\ell-1}$  if and only if  $f(x)$  can be written as a function of the first  $\ell$  digits of  $x$ , so that  $f(x) = g(x_0, x_1, \dots, x_{\ell-1})$  for some  $g : (\mathbb{Z}/p\mathbb{Z})^\ell \rightarrow \mathbb{Z}/p\mathbb{Z}$ ;

(ii)  $f(x)$  depends only on  $x_\ell$  (that is,  $f(x) = g(x_\ell)$  for some function  $g$ ) if and only if  $f \in \text{span}\{\phi_0, \phi_{p^\ell}, \phi_{2p^\ell}, \dots, \phi_{(p-1)p^\ell}\}$ .

(iii) if  $f(x) = g(x_\ell)$  for a function  $g$  of degree  $m \in [p]$ , then  $f \in \text{span}\{\phi_0, \phi_{p^\ell}, \phi_{2p^\ell}, \dots, \phi_{mp^\ell}\}$ .

*Proof.* We prove (i), the proof of (ii) being similar. Suppose that  $f$  has degree at most  $p^\ell - 1$ . Then  $f$  is a linear combination of functions  $\phi_m(x)$  with  $m \leq p^\ell - 1$ , so that  $m_i = 0$  for all  $i \geq \ell$ . By (3.4),  $f$  depends only on  $x_0, x_1, \dots, x_{\ell-1}$ .

To prove the converse implication, we use dimension counting. There are  $p^\ell$  functions  $\phi_m$  with  $m \leq p^\ell - 1$ , all linearly independent, so that  $\Omega_{p^\ell-1}$  has dimension  $p^\ell$ . On the other hand, the space of all functions of  $x_0, x_1, \dots, x_{\ell-1}$  also has dimension  $p^\ell$ , since that is the number of all  $\ell$ -tuples  $(x_0, x_1, \dots, x_{\ell-1}) \in (\mathbb{Z}/p\mathbb{Z})^\ell$ . This proves (i).

For (iii), assume that  $g = \phi_j$  for some  $j \leq m \leq p - 1$ . Then

$$f(x) = g(x_\ell) = \binom{x_\ell}{j} = \binom{x}{jp^\ell} = \phi_{jp^\ell}(x)$$

by the definition of the phi functions and by Lucas' theorem, and (iii) follows.  $\square$

**Lemma 4.6.** *Let  $\ell, m \in \mathbb{Z}_{\geq 0}$ . Then  $\phi_\ell \cdot \phi_m \in \Omega_{\ell+m}$ , with*

$$(4.4) \quad \phi_\ell \cdot \phi_m =_{\ell+m-1} \binom{\ell+m}{\ell} \phi_{\ell+m}.$$

We emphasize that  $\phi_\ell \cdot \phi_m$  has degree *at most*  $\ell + m$  but not necessarily equal to it, since the coefficient of  $\phi_{\ell+m}$  in (4.4) could be zero. For example, if  $\ell, m \leq p^j - 1$  for some  $j < k$ , then, by Lemma 4.5 (i), both  $\phi_\ell(x)$  and  $\phi_m(x)$  depend only on the first  $j$   $p$ -adic digits of  $x$ . Therefore so does  $\phi_\ell(x)\phi_m(x)$ . By Lemma 4.5 (i) again,  $\phi_\ell\phi_m$  also has degree at most  $p^j - 1$ , even if  $\ell + m \geq p^j$ .

*Proof of Lemma 4.6.* We prove (4.4) by induction on  $K := \ell + m$ . If  $K = 0$ , then  $\ell = m = 0$  and the formula is immediate. Assume now that the formula is true for all  $\ell, m$  with  $\ell + m = K$  for some  $K \geq 0$ , and consider the case  $\ell + m = K + 1$ . Then, by (3.3) and the inductive

assumption,

$$\begin{aligned}
D(\phi_\ell \cdot \phi_m)(x) &= \phi_\ell(x+1)\phi_m(x+1) - \phi_\ell(x)\phi_m(x) \\
&= (\phi_\ell(x+1) - \phi_\ell(x))\phi_m(x+1) + \phi_\ell(x)(\phi_m(x+1) - \phi_m(x)) \\
&= \phi_{\ell-1}(x)(\phi_m(x) + \phi_{m-1}(x)) + \phi_\ell(x)\phi_{m-1}(x) \\
&=_{\ell+m-2} \left[ \binom{\ell+m-1}{\ell-1} + \binom{\ell+m-1}{\ell} \right] \phi_{\ell+m-1} \\
&= \binom{\ell+m}{\ell} \phi_{\ell+m-1},
\end{aligned}$$

where at the last step we used Pascal's identity. On the other hand, by (4.2) we also have  $D\left(\binom{\ell+m}{\ell}\phi_{\ell+m}\right) = \binom{\ell+m}{\ell}\phi_{\ell+m-1}$ . Hence

$$D\left(\phi_\ell \cdot \phi_m - \binom{\ell+m}{\ell}\phi_{\ell+m}\right) \in \Omega_{\ell+m-2},$$

and (4.4) follows from (4.3).  $\square$

**Lemma 4.7.** *Let  $\phi_m : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  and  $b \in R^\times$ . Then*

$$\phi_m(bx) =_{m-1} b^m \phi_m(x)$$

*Proof.* We induct on  $m$ . The case  $m = 0$  is immediate, since  $\phi_0$  is a constant function. Assume now that the result holds for  $m \leq \ell$ . We consider  $m = \ell + 1$ . Let  $\phi_m^b$  be the function defined by  $\phi_m^b(x) = \phi_m(bx)$ . Then by (3.5),

$$\begin{aligned}
D\phi_{\ell+1}^b(x) &= \phi_{\ell+1}(bx+b) - \phi_{\ell+1}(bx) \\
&= \sum_{j=0}^{\ell} \phi_{\ell+1-j}(b)\phi_j(bx) \\
&=_{\ell-1} b\phi_\ell(bx),
\end{aligned}$$

where at the last step we used that  $\phi_1(b) = b$ . By the inductive hypothesis with  $m = \ell$ , we have

$$D\phi_{\ell+1}^b(x) =_{\ell-1} b^{\ell+1}\phi_\ell(x).$$

But we also have  $D(b^{\ell+1}\phi_{\ell+1})(x) = b^{\ell+1}\phi_\ell(x)$  by (4.2), so that

$$D(b^{\ell+1}\phi_{\ell+1} - \phi_{\ell+1}^b) \in \Omega_{\ell-1}.$$

The inductive step follows from this and (4.3).  $\square$

The next lemma is a phi-function analogue of the fact that the coefficients of a polynomial can be computed by evaluating its derivatives at 0.

**Lemma 4.8.** *Suppose that  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  has the representation  $f = \sum_{j=0}^{p^k-1} c_j \phi_j$ . Then*

$$(4.5) \quad c_\ell = D^\ell f(0) \text{ for all } \ell \in [p^k].$$

*Proof.* By (4.2), we have

$$D^\ell f = \sum_{j=\ell}^{p^k-1} c_j \phi_{j-\ell}.$$

We now evaluate this at  $x = 0$ . Since  $\phi_0(0) = 1$  and  $\phi_j(0) = 0$  for all  $j > 0$ , we get (4.5).  $\square$

**Corollary 4.9.** *Let  $a \in R$  and  $m \in [p^k]$ . Then*

$$\phi_m(ax) = \sum_{\ell=0}^m A_{m,\ell}(a) \phi_\ell(x),$$

where  $A_{m,\ell}(a) = \Delta_a^\ell \phi_m(0)$ .

*Proof.* For  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  and  $a \in R$ , define  $f^a(x) = f(ax)$ . Then  $(Df^a)(x) = f(ax + a) - f(ax) = (\Delta_a f)(ax)$ , and, by iteration,

$$(4.6) \quad (D^\ell f^a)(x) = (\Delta_a^\ell f)(ax) \text{ for all } \ell \in [p^k].$$

The corollary follows by applying Lemma 4.8 to  $f = \phi_m^a$  and then using (4.6).  $\square$

## 5. PHI FUNCTIONS ON $R^n$

**5.1. Phi functions as generalized polynomials.** For  $\alpha = (\alpha_1, \dots, \alpha_n) \in [p^k]^n$ , we define  $\phi_\alpha : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  by

$$\phi_\alpha(x) = \phi_{\alpha_1}(x_1) \cdots \phi_{\alpha_n}(x_n).$$

Let also

$$\Omega_m^n := \text{span}\{\phi_\alpha : |\alpha| \leq m\},$$

where  $|\alpha| = \sum_i \alpha_i$ . We say that a function  $f : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  has *degree at most  $m$*  if  $f \in \Omega_m^n$ . By convention, we set  $\Omega_m^n := \{0\}$  for  $m < 0$ .

**Lemma 5.1.** *The functions  $\{\phi_\alpha : \alpha \in [p^k]^n\}$  are linearly independent over  $\mathbb{Z}/p\mathbb{Z}$ .*

*Proof.* We induct on  $n$ . The case  $n = 1$  is given by Lemma 3.4. Assume now that  $n > 1$  and that the lemma holds in dimensions less than  $n$ . Suppose that there exist  $c_\alpha \in \mathbb{Z}/p\mathbb{Z}$  such that

$$\sum_{\alpha \in [p^k]^n} c_\alpha \phi_\alpha(x_1, \dots, x_n) = 0.$$

Write  $\alpha = (\tilde{\alpha}, \alpha_n)$ , where  $\tilde{\alpha} = (\alpha_1, \dots, \alpha_{n-1})$ . For fixed  $x_1, \dots, x_{n-1} \in R$ , we have

$$0 = \sum_{\alpha_n=0}^{p^k-1} \left( \sum_{\tilde{\alpha} \in [p^k]^{n-1}} c_{(\tilde{\alpha}, \alpha_n)} \phi_{\tilde{\alpha}}(x_1, \dots, x_{n-1}) \right) \phi_{\alpha_n}(x_n).$$

This is true for all  $x_n \in R$ , so by the linear independence of the functions  $\phi_{\alpha_n}$ , we have

$$\sum_{\tilde{\alpha} \in [p^k]^{n-1}} c_{(\tilde{\alpha}, \alpha_n)} \phi_{\tilde{\alpha}}(x_1, \dots, x_{n-1}) = 0$$

for all  $\alpha_n$ . Since this holds for all  $x_1, \dots, x_{n-1} \in R$ , it follows by the inductive hypothesis that  $c_{(\tilde{\alpha}, \alpha_n)} = 0$  for all  $\tilde{\alpha}, \alpha_n$ . That is,  $c_\alpha = 0$  for all  $\alpha$ .  $\square$

**Corollary 5.2.** *For  $m \leq p^k - 1$ , the dimension of  $\Omega_m^n$  over  $\mathbb{Z}/p\mathbb{Z}$  is  $\binom{m+n}{n}$ .*

*Proof.* By Lemma 5.1, the functions  $\phi_\alpha$  with  $|\alpha| \leq m$  are linearly independent. Therefore the dimension of  $\Omega_m^n$  over  $\mathbb{Z}/p\mathbb{Z}$  is equal to the number of  $\alpha \in [p^k]^n$  such that  $|\alpha| \leq m$ . By Lemma 5.3 below, this number is equal to  $\binom{m+n}{n}$ .  $\square$

**Lemma 5.3.** *Let  $M, L \in \mathbb{N}$  and suppose that  $L < M$ . Then*

$$\#\{(\ell_1, \dots, \ell_n) \in [M]^n : \ell_1 + \dots + \ell_n \leq L\} = \binom{L+n}{n}.$$

*Proof.* What we seek is equivalent to the number of  $(n+1)$ -tuples  $(\ell_1, \dots, \ell_{n+1}) \in [M]^{n+1}$  such that  $\ell_1 + \dots + \ell_{n+1} = L$ . By a stars and bars combinatorial argument, there are  $\binom{L+n}{n}$  such tuples.  $\square$

**Definition 5.4. (Iterated differences)** *Let  $f : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  be a function. For  $r \in R^n$ , define*

$$\Delta_r f(x) := f(x+r) - f(x).$$

*The iterated difference function of  $f$  of order  $d \in \mathbb{N}$  with steps  $r^{(1)}, \dots, r^{(d)} \in R^n$  is*

$$(5.1) \quad \Delta_{r^{(1)}} \dots \Delta_{r^{(d)}} f(x) = \sum_{\vec{\epsilon} \in \{0,1\}^d} (-1)^{|\epsilon|+d} f(x_{\vec{\epsilon}}),$$

*where for each  $\vec{\epsilon} = (\epsilon_1, \dots, \epsilon_d) \in \{0,1\}^d$ ,*

$$|\epsilon| = \sum_{j=1}^d \epsilon_j, \quad x_{\vec{\epsilon}} = x + \sum_{j=1}^d \epsilon_j r^{(j)}.$$

*We say that a function  $f : R^n \rightarrow R$  is  $d$ -null if  $\Delta_{r^{(1)}} \dots \Delta_{r^{(d)}} f(x) = 0$  for all  $x$  and for all  $r^{(1)}, \dots, r^{(d)} \in R^n$ .*

It is useful to think of  $\Delta_{r^{(1)}} \dots \Delta_{r^{(d)}} f(x)$  as the evaluation of  $f$  on the  $d$ -dimensional box with vertices  $x_{\vec{\epsilon}}$ , where the values of  $f(x_{\vec{\epsilon}})$  are counted with alternating  $\pm$  signs as indicated. Note that the differences  $r^{(j)}$  need not be distinct, in which case some of the vertices may occur in (5.1) for more than one value of  $\vec{\epsilon}$ .

In Proposition 5.6 below, we show that a function  $f : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  is  $(d+1)$ -null if and only if  $f \in \Omega_d^n$ . First, we need the following lemma.

**Lemma 5.5.** *For  $\alpha \in [p^k]^n$  and  $r \in R^n$ , we have  $\Delta_r \phi_\alpha \in \Omega_{|\alpha|-1}^n$ .*

*Proof.* We induct on  $n$ . When  $n = 1$ , the result is true by Lemma 4.3. Now assume that  $n > 1$ , and that the lemma holds in all dimensions lower than  $n$ . Then

$$\begin{aligned} \phi_\alpha(x+r) - \phi_\alpha(x) &= \prod_{j=1}^n \phi_{\alpha_j}(x_j+r_j) - \prod_{j=1}^n \phi_{\alpha_j}(x_j) \\ &= (\Delta_{r_1} \phi_{\alpha_1}(x_1)) \phi_{(\alpha_2, \dots, \alpha_n)}(x_2, \dots, x_n) \\ &\quad + \phi_{\alpha_1}(x_1+r_1) \Delta_{(r_2, \dots, r_n)} \phi_{(\alpha_2, \dots, \alpha_n)}(x_2, \dots, x_n). \end{aligned}$$

By the inductive assumption, we have

$$\Delta_{r_1} \phi_{\alpha_1}(x_1) \in \Omega_{\alpha_1-1}^1, \quad \Delta_{(r_2, \dots, r_n)} \phi_{(\alpha_2, \dots, \alpha_n)} \in \Omega_{\alpha_2 + \dots + \alpha_n - 1}^{n-1},$$

where we recall that  $f \in \Omega_{-1}^n$  means that  $f$  is the zero function. Additionally,  $\phi_{\alpha_1}(x_1+r_1) \in \Omega_{\alpha_1}$  by (3.5). It follows that  $\Delta_r \phi_\alpha \in \Omega_{|\alpha|-1}^n$ , as claimed.  $\square$

**Proposition 5.6.** *Let  $g : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  and  $d \in \{0, 1, \dots, n(p^k - 1)\}$ . Then  $g$  is  $(d+1)$ -null if and only if  $g \in \Omega_d^n$ .*



*Proof.* It follows by iterating Lemma 5.5 that functions in  $\Omega_d^n$  are  $(d+1)$ -null. We need to prove the converse: if  $g$  is  $(d+1)$ -null, then  $g \in \Omega_d^n$ . We induct on  $n$ , and within the induction on  $n$ , induct on  $d$ . For the base case  $n = 1$ , the argument below works; we just need to ignore the presence of the  $\tilde{x}$ .

The claim is true for any  $n$  when  $d = 0$ , since any 1-null function is constant. Assume now that the claim is true in all dimensions lower than  $n$ , and true for  $d$ -null functions in  $R^n$  for some  $d \geq 0$ .

Let  $g : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  be  $(d+1)$ -null. Define  $h(x) = g(x + e_n) - g(x - e)$ , where  $e_n$  is the vector with a 1 in the  $n^{\text{th}}$  coordinate, and 0s otherwise. For  $x \in R^n$ , we will write  $x = (x_1, \dots, x_n) =: (\tilde{x}, x_n)$ , where  $\tilde{x} = (x_1, \dots, x_{n-1})$ . Then

$$(5.2) \quad g(x) = g(\tilde{x}, 0) + h(\tilde{x}, 0) + h(\tilde{x}, 1) + \dots + h(\tilde{x}, x_n - 1).$$

The function  $\tilde{g}(\tilde{x}) = g(\tilde{x}, 0)$ , considered as a function on  $R_{\tilde{x}}^{n-1}$ , is  $(d+1)$ -null. By the lower-dimensional part of the inductive assumption, we have  $\tilde{g} \in \Omega_d^{n-1}$ . Considering now  $g(\tilde{x}, 0)$  as a function of  $n$  variables that is constant in the  $e_n$  direction, we have

$$g(\tilde{x}, 0) = \tilde{g}(\tilde{x})\phi_0(x_n) \in \Omega_d^n.$$

Next,  $h = \Delta_{e_n}g$  is  $d$ -null. By the inductive hypothesis on  $d$ , we can write

$$h(x) = \sum_{\beta \in [p^k]^{n-1}, |\beta| \leq d-1} \phi_\beta(\tilde{x}) \sum_{j=0}^{d-1-|\beta|} a_{\beta,j} \phi_j(x_n).$$

so that

$$\begin{aligned} \sum_{\ell=1}^{x_n} h(\tilde{x}, \ell) &= \sum_{\ell=1}^{x_n} \sum_{|\beta| \leq d-1} \phi_\beta(\tilde{x}) \sum_{j=0}^{d-1-|\beta|} a_{\beta,j} \phi_j(\ell) \\ &= \sum_{|\beta| \leq d-1} \phi_\beta(\tilde{x}) \sum_{j=0}^{d-1-|\beta|} a_{\beta,j} \sum_{\ell=1}^{x_n} \phi_j(\ell) \\ &= \sum_{|\beta| \leq d-1} \sum_{j=0}^{d-1-|\beta|} a_{\beta,j} \phi_\beta(\tilde{x}) \phi_{j+1}(x_n). \end{aligned}$$

But for each pair  $\beta, j$  appearing in the sum,

$$\phi_\beta(\tilde{x})\phi_{j+1}(x_n) = \phi_{(\beta, j+1)}(x) \in \Omega_d^n.$$

This ends the proof of the proposition.  $\square$

**Corollary 5.7.** *Let  $g : R^n \rightarrow \mathbb{Z}/p\mathbb{Z}$  and  $d \in \{0, 1, \dots, p-1\}$ . Then  $g \in \Omega_d^n$  if and only if  $g$  is a polynomial in  $R[x_1, \dots, x_n]$  of degree at most  $d$ .*

In particular, since  $\{\phi_\alpha : |\alpha| \leq d\}$  is a basis for  $\Omega_d^n$ , it follows that each  $\phi_\alpha$  with  $|\alpha| \leq p-1$  is a polynomial of degree  $|\alpha|$ .

*Proof.* It is well known, and easy to check directly, that if  $f$  is a polynomial of degree  $d$  then  $\Delta_c f$  is a polynomial of degree at most  $d-1$  for any  $c \in R$ . By iteration, it follows that every polynomial  $g$  of degree  $d \leq p-1$  is  $(d+1)$ -null. By Proposition 5.6, we have  $g \in \Omega_d^n$ .

Moreover,  $\Omega_d^n$  and the space of all polynomials in  $R[x_1, \dots, x_n]$  of degree at most  $d$  have the same dimension  $\binom{d+n}{n}$  (the number of distinct multiindices  $\alpha = (\alpha_1, \dots, \alpha_n)$  with  $|\alpha| \leq d$ ; see Lemma 5.3 above). Therefore the two spaces are equal.  $\square$

**5.2. Phi functions and hyperplanes.** Recall that

$$(5.3) \quad \mathcal{H}^n := \text{span}\{\mathbf{1}_{H_b(a)} : a \in R^n, b \in \mathbb{P}R^{n-1}\}$$

is the linear span of indicator functions of affine hyperplanes. We will refer to functions in  $\mathcal{H}^n$  as *hyperplane functions* in  $R^n$ .

We are interested in characterizing hyperplane functions and, in particular, determining the dimension of  $\mathcal{H}^n$ . To this end, we first find a spanning set in terms of the phi functions.

**Lemma 5.8.** *We have*

$$\mathcal{H}^n = \text{span}\{\phi_\ell(\langle x, b \rangle) : \ell \in [p^k], b \in \mathbb{P}R^{n-1}\}.$$

*Proof.* It suffices to prove that for each  $b \in \mathbb{P}R^{n-1}$ ,

$$(5.4) \quad \begin{aligned} \text{span}\{\mathbf{1}_{H_b(a)} : a \in R\} &= \text{span}\{f(\langle x, b \rangle) : f \in (\mathbb{Z}/p\mathbb{Z})^R\} \\ &= \text{span}\{\phi_\ell(\langle x, b \rangle) : \ell \in [p^k]\}. \end{aligned}$$

The second equality in (5.4) follows from Lemma 3.4. We now prove the first one. For any  $b \in \mathbb{P}R^{n-1}$  and  $a \in R$ , we may write

$$\mathbf{1}_{H_b(a)}(x) = \mathbf{1}_{\{0\}}(\langle x - a, b \rangle) = \mathbf{1}_{\{a, b\}}(\langle x, b \rangle)$$

which shows that  $\mathbf{1}_{H_b(a)}$  can be written as a single-variable function of  $\langle x, b \rangle$  as claimed. Conversely, let  $f : R \rightarrow \mathbb{Z}/p\mathbb{Z}$  be a function. Then

$$f(x) = \sum_{c \in R} f(c) \mathbf{1}_{\{c\}}, \text{ hence } f(\langle x, b \rangle) = \sum_{c \in R} f(c) \mathbf{1}_{\{c\}}(\langle x, b \rangle)$$

Since  $b \in \mathbb{P}R^{n-1}$ , there exists  $i \in \{1, 2, \dots, n\}$  such that  $b_i$  is invertible. For each  $c \in R$ , let  $\bar{c} \in R^n$  be the vector whose  $i$ -th coordinate is  $cb_i^{-1}$  and all other coordinates are 0. Then  $\langle \bar{c}, b \rangle = c$ , so that

$$\mathbf{1}_{\{c\}}(\langle x, b \rangle) = \mathbf{1}_{H_b(\bar{c})}(x).$$

Hence every function  $f(\langle x, b \rangle)$  can be written as a linear combination of hyperplane functions with the normal vector  $b$ . This ends the proof of (5.4), and of the lemma.  $\square$

**Proposition 5.9.** *We have  $\mathcal{H}^n \subset \Omega_{p^k-1}^n$  for all  $k \geq 1$ . Moreover, if  $k = 1$  then  $\mathcal{H}^n = \Omega_{p-1}^n$ . In particular,*

$$(5.5) \quad \text{rank}(\mathcal{A}_{p^k, n}^*) = \dim(\mathcal{H}^n) \leq \binom{p^k - 1 + n}{n},$$

and (5.5) holds with equality when  $k = 1$ .

*Proof of Proposition 5.9, part 1.* We prove that  $\mathcal{H} \subset \Omega_{p^k-1}^n$  for all  $k \geq 1$ . By Lemma 5.8, it suffices to prove that  $\phi_\ell(\langle b, x \rangle) \in \Omega_\ell^n$  for all  $\ell \in [p^k]$  and  $b \in \mathbb{P}R^{n-1}$ . To this end, we use (3.5) to write

$$(5.6) \quad \phi_\ell(\langle b, x \rangle) = \sum_{|\alpha| \leq \ell} \phi_{\alpha_1}(b_1 x_1) \cdots \phi_{\alpha_n}(b_n x_n).$$

But Lemma 4.7 implies that  $\phi_{\alpha_i}(b_i \cdot) \in \Omega_{\alpha_i}$  for each  $i$ . Hence each term on the right side of (5.6) has degree at most  $|\alpha|$ , which in turn implies that  $\phi_\ell(\langle b, x \rangle) \in \Omega_\ell^n$  as claimed. The bound (5.5) follows from Corollary 5.2 with  $m = p^k - 1$ .  $\square$

The proof of the converse inclusion for  $k = 1$  will be based on the two lemmas below. For  $d \in [p]$ , let  $\mathcal{P}_{\leq d}^n := (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]_{\leq d}$  be the space of polynomials in  $n$  variables of degree at most  $d$  over  $\mathbb{Z}/p\mathbb{Z}$ , and let  $\mathcal{P}_{=d}^n$  be the subspace of homogeneous, degree  $d$  polynomials in  $\mathcal{P}_{\leq d}^n$ . The relation between polynomials and hyperplane indicator functions for  $k = 1$  is well understood in the literature, see [11, 14, 16]. The proof below is provided for completeness.

**Lemma 5.10.** *Let  $k = 1$ . For any  $n \in \mathbb{N}$  and any  $d \in \{0, 1, \dots, p-1\}$ ,*

$$\text{span} \{ \langle x, b \rangle^d : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^n \} = \mathcal{P}_{=d}^n.$$

*Proof.* We proceed with induction on  $n$ . The case  $n = 1$  is immediate. Suppose that the statement holds in all dimensions lower than  $n$ . We show that

$$x^\alpha \in \text{span} \{ \langle x, b \rangle^d : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1} \}$$

for all  $\alpha \in [p]^n$  with  $|\alpha| = d$ .

For  $x \in (\mathbb{Z}/p\mathbb{Z})^n$ , we write  $x = (\tilde{x}, x_n)$ , where  $\tilde{x} = (x_1, \dots, x_{n-1})$ . Write also  $\alpha = (\beta, \alpha_n)$ , where  $\beta = (\alpha_1, \dots, \alpha_{n-1})$ , so that  $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} = \tilde{x}^\beta x_n^{\alpha_{k+1}}$ . Let  $\ell = |\beta|$ . By the inductive hypothesis, we may write

$$\tilde{x}^\beta x_n^{\alpha_n} = \sum_{c \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-2}} a_c \langle \tilde{x}, c \rangle^\ell x_n^{\alpha_n}.$$

Therefore it suffices to show that

$$\langle \tilde{x}, c \rangle^\ell x_n^{\alpha_n} \in \text{span} \{ \langle x, b \rangle^d : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1} \}$$

for all  $c \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-2}$ . To this end, it is enough to prove that

$$(5.7) \quad \{ \langle \tilde{x}, c \rangle^j x_n^{d-j} : j = 0, 1, \dots, d-1 \} \subset \text{span} \{ \langle x, (c, i) \rangle^d - (ix_n)^d : i = 1, \dots, d \},$$

where  $(c, i) = (c_1, \dots, c_{n-1}, i) \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}$ . Note that

$$\langle x, (c, i) \rangle^d - (ix_n)^d = \sum_{j=0}^{d-1} \binom{d}{j} i^j \langle \tilde{x}, c \rangle^{d-j} x_n^j.$$

We consider this as a system of  $d$  linear equations with  $\langle \tilde{x}, c \rangle^{d-j} x_n^j$ . The coefficient matrix of this system has the determinant

$$\left( \prod_{j=0}^{d-1} \binom{d}{j} \right) \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{d-1} \\ \vdots & & & & \\ 1 & d & d^2 & \cdots & d^{d-1} \end{pmatrix} = \prod_{j=0}^{d-1} \binom{d}{j} \prod_{1 \leq i < j \leq d} (i - j),$$

where we evaluated the determinant of the Vandermonde matrix. Since  $\binom{d}{j} \neq 0$  for  $d \leq p-1$ , our coefficient matrix is nonsingular, so that we can solve for  $\langle \tilde{x}, c \rangle^{d-j} x_n^j$  as claimed in (5.7).  $\square$

**Lemma 5.11.** *Let  $k = 1$ . For any  $d \in \{0, 1, \dots, p-1\}$ , we have*

$$\text{span} \{ \langle x - a, b \rangle^d : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}, a \in (\mathbb{Z}/p\mathbb{Z})^n \} = \mathcal{P}_{\leq d}^n.$$

*Proof.* By Lemma 5.10, it suffices to show that

$$\text{span}\{\langle x - a, b \rangle^d : a \in (\mathbb{Z}/p\mathbb{Z})^n\} = \text{span}\{\langle x, b \rangle^\ell : \ell \in \mathbb{N}, \ell \leq d\}.$$

For any  $a \notin H_b$ , we know that  $\langle a, b \rangle$  is non-zero, and so a unit. Then  $\langle ca, b \rangle$  will range over all values in  $\mathbb{Z}/p\mathbb{Z}$  as  $c$  ranges over all values in  $\mathbb{Z}/p\mathbb{Z}$ . Consequently,

$$\{\langle x - a, b \rangle^d : a \in (\mathbb{Z}/p\mathbb{Z})^n\} = \{(\langle x, b \rangle - c)^d : c = 0, \dots, p-1\}.$$

Consider the system of equations

$$(\langle x, b \rangle - c)^d = \sum_{j=0}^d \binom{d}{j} c^j \langle x, b \rangle^{d-j}, \quad c = 0, \dots, d,$$

with  $\langle x, b \rangle^{d-j}$  as the unknowns. The coefficient matrix of this system has the determinant

$$\left( \prod_{j=0}^d \binom{d}{j} \right) \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^d \\ \vdots & & & & \\ 1 & d & d^2 & \cdots & d^d \end{pmatrix} = \prod_{j=0}^d \binom{d}{j} \prod_{c=2}^d c \prod_{1 \leq u < v \leq d} (u - v).$$

This is non-zero as in the proof of Lemma 5.10, hence we can solve for  $\langle x, b \rangle^{d-j}$ . □

*Proof of Proposition 5.9, part 2.* Assume that  $k = 1$ . Observe that the characteristic function of a hyperplane  $H_b(a)$  may be written as  $\mathbf{1}_{H_b(a)}(x) = 1 - \langle x - a, b \rangle^{p-1} \pmod{p}$ . By Lemma 5.11 with  $d = p - 1$ , we have  $\mathcal{H}^n = \mathcal{P}_{\leq p-1}^n$ . It follows by Corollary 5.7 that  $\mathcal{H}^n = \Omega_{p-1}^n$ , as claimed. □

**Remark 5.1.** Let  $\mathcal{H}_0^n = \text{span}\{\mathbf{1}_{H_b} : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}\}$  be the span of homogeneous hyperplane functions. The same argument as above, but using Lemma 5.10 instead of 5.11, shows that  $\mathcal{H}_0^n$  is spanned by homogeneous polynomials of degree  $p - 1$  together with  $\mathbf{1}_{(\mathbb{Z}/p\mathbb{Z})^n}$ , the function identically equal to 1. To prove the converse, it suffices to verify that  $\mathbf{1}_{(\mathbb{Z}/p\mathbb{Z})^n}$  can be represented as a linear combination of hyperplane functions. Such representation is provided by

$$\mathbf{1}_{(\mathbb{Z}/p\mathbb{Z})^n} = \mathbf{1}_{x_1=0} + \sum_{c=0}^{p-1} \mathbf{1}_{x_2=cx_1}.$$

This offers a proof of Theorem 1.2.

## 6. DEGREE LOWERING FOR PRODUCTS

**Lemma 6.1.** Let  $f(x, y) = \phi_m(x_i y_j)$  for some  $m \in [p^k]$  and  $i, j \geq 1$ , where  $x = \sum x_\ell p^\ell$  and  $y = \sum y_\ell p^\ell$  are the  $p$ -adic expansions of  $x, y \in R$ . Then  $f$  has degree at most  $mp^{i+j}$ , with equality attained only when  $p = 2$  and  $i = j = m = 1$ .

*Proof.* By Lemma 4.5 (ii), we have

$$f(x, y) = \sum_{\alpha} c_{\alpha} \phi_{\alpha_1}(x) \phi_{\alpha_2}(y),$$

where the summation is over  $\alpha = (\alpha_1, \alpha_2)$  with

$$\alpha_1 \in \{0, p^i, 2p^i, \dots, (p-1)p^i\}, \quad \alpha_2 \in \{0, p^j, 2p^j, \dots, (p-1)p^j\}.$$

Thus the combined degree of each  $\phi_{\alpha_1}(x)\phi_{\alpha_2}(y)$  is at most  $(p-1)p^i + (p-1)p^j = p^{i+1} + p^{j+1} - p^i - p^j$ . We may assume that  $i \leq j$ .

- If  $i < j$ , then  $p^{i+1} \leq p^j$ , so that  $p^{i+1} + p^{j+1} - p^i - p^j \leq p^{j+1} - p^i < p^{i+j}$ .
- If  $i = j \geq 2$ , then  $2p^{i+1} - 2p^i < 2p^{i+1} \leq p^{i+2} \leq p^{i+j}$ .
- If  $i = j = 1$ , then  $2p^2 - 2p < 2p^2 = 2p^{i+j}$ . This is at most  $mp^{i+j}$  unless  $m = 1$ . However, if  $m = 1$ , then

$$\phi_1(x_1y_1) = x_1y_1 = \phi_p(x)\phi_p(y)$$

has degree  $2p \leq p^2$ , with equality only when  $p = 2$ .

□

Our next goal is to determine the degree of  $f(x, y) = \phi_m(xy)$  as a function of 2 variables for  $m \in [p^k]$ . Recall from Corollary 4.9 that

$$(6.1) \quad \phi_m(xy) = \sum_{\ell=0}^m A_{m,\ell}(y) \phi_\ell(x),$$

where  $A_{m,\ell}(y) = \Delta_y^\ell \phi_m(0) = \sum_{i=0}^\ell (-1)^{i+\ell} \binom{\ell}{i} \phi_m(iy)$ . By Lemma 4.7,  $\phi_m(iy)$  is a function of degree at most  $m$  in  $y$  for each  $i$ . Hence  $\phi_m(xy)$  has degree at most  $m$  in each variable separately.

We will see below that the *combined* degree of  $\phi_m(xy)$ , considered as a function of two variables, cannot be much larger than  $m$ . This is in sharp contrast to polynomials over  $\mathbb{Z}$ , where the combined degree of  $(xy)^m = x^m y^m$  is always  $2m$ .

**Proposition 6.2.** *Let  $f(x, y) = \phi_m(xy)$  for some  $m \in [p^k]$  and  $x, y \in R$ . Then  $f$  has degree at most  $m + 2(p-1)$ . Specifically, we have*

$$(6.2) \quad \phi_m(xy) = \sum_{\alpha} c_{m,\alpha} \phi_{\alpha_1}(x)\phi_{\alpha_2}(y),$$

where the coefficients  $c_{m,\alpha}$  satisfy  $c_{m,\alpha} = 0$  if  $|\alpha| > m + 2(p-1)$ .

*Proof.* Let  $m \in [p^k]$ , and let  $x = \sum x_i p^i$  and  $y = \sum y_i p^i$  be the  $p$ -adic expansions of  $x, y \in R$ . By (3.5) and Lemma 3.6, we have

$$\begin{aligned} \phi_m(xy) &= \phi_m \left( \sum_{i+j \leq k-1} p^{i+j} x_i y_j \right) \\ &= \sum_{\vec{m}} \prod_{i,j} \phi_{m_{ij}}(x_i y_j), \end{aligned}$$

where the summation is over all  $\vec{m} = (m_{ij})_{i+j \leq k-1}$  such that  $\sum_{i,j} m_{ij} p^{i+j} = m$ . Fix  $\vec{m}$ , and consider the corresponding term in the sum above:

$$\begin{aligned} \prod_{i,j} \phi_{m_{ij}}(x_i y_j) &= \left( \prod_{j=0}^{k-1} \phi_{m_{0j}}(x_0 y_j) \right) \left( \prod_{i=0}^{k-1} \phi_{m_{i0}}(x_i y_0) \right) \left( \prod_{i,j \geq 1} \phi_{m_{ij}}(x_i y_j) \right) \\ &=: P_1 P_2 P_3, \end{aligned}$$

By Lemma 6.1,  $P_3$  has degree at most

$$(6.3) \quad \sum_{i,j \geq 1} m_{ij} p^{i+j}.$$

Next, we consider  $P_1$ . By (6.1) and Lemma 4.5, each factor  $\phi_{m_{0j}}(x_0 y_j)$  has degree at most  $p-1$  in  $x$  and at most  $m_{0j}$  in  $y_j$ , therefore at most  $m_{0j} p^j$  in  $y$ . In other words, we can write  $\phi_{m_{0j}}(x_0 y_j)$  as a linear combination of terms of the form  $\phi_{\beta_1}(x_0) \phi_{\beta_2}(y)$ , where  $\beta_2 \leq m_{0j} p^j$ . Taking the product, and applying Lemma 4.5 to the factors involving  $x_0$  and Lemma 4.6 to the factors involving  $y$ , we see that  $P_1$  has degree at most

$$(6.4) \quad (p-1) + \sum_j m_{0j} p^j.$$

Similarly,  $P_2$  has degree at most  $(p-1) + \sum_i m_{i0} p^i$ . Combining this with (6.3) and (6.4), we get the desired bound.  $\square$

## 7. AN UPPER BOUND ON THE RANK OF HYPERPLANE FUNCTIONS

In this section we prove our lower bound on the rank of the reduced point-affine hyperplane incidence matrix, which we state again for the reader's convenience.

**Theorem 7.1.** *Let  $p$  be prime, and let  $k, n \in \mathbb{N}$ . Then*

$$(7.1) \quad \text{rank}(\mathcal{A}_{p^k, n}^*) \leq (2n) \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n}.$$

Before starting the proof of the theorem, we compare (7.1) to the upper bound  $\binom{p^k-1+n}{n}$  given by (5.5). Suppose that  $n$  is small relative to  $p^{k-1}$ , with  $n < \epsilon p^{k-1}$  for some  $\epsilon > 0$ . Then

$$(2n) \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n} \leq \frac{(p^k + 2(n-1)(p-1) + 2n)^n}{2^{n-1}(n-1)!} < \frac{p^{kn}(1+4\epsilon)^n}{2^{n-1}(n-1)!}.$$

Meanwhile, we have

$$\binom{p^k - 1 + n}{n} \geq \frac{p^{kn}}{n!}.$$

Hence, for  $n < \epsilon p^{k-1}$ , the estimate in (7.1) improves on that in Proposition 5.5 by a factor of at least  $n 2^{-(n-1)} (1+4\epsilon)^n$ .

*Proof of Theorem 7.1.* Recall that the rows of  $\mathcal{A}_{p^k, n}^*$  are given by indicator functions of hyperplanes  $H_b(a)$  with  $a \in R^n$  and  $b \in \mathbb{P}R^{n-1}$ . Hence its rank is equal to the dimension of  $\mathcal{H}^n$  over  $\mathbb{Z}/p\mathbb{Z}$ , where  $\mathcal{H}^n$  was defined in (5.3). By Lemma 5.8, we further have

$$(7.2) \quad \mathcal{H}^n = \text{span}\{\phi_\ell(\langle x, b \rangle) : \ell \in [p^k], b \in \mathbb{P}R^{n-1}\}.$$

Any  $b \in \mathbb{P}R^{n-1}$  has a representative in  $R^n$  with at least one component equal to 1. Hence

$$(7.3) \quad \text{rank}(\mathcal{A}_{p^k, n}^*) \leq n \cdot \text{rank}(\mathbb{H}^{(n)}),$$

where  $\mathbb{H}^{(n)}$  is the matrix with rows indexed by  $(m, \tilde{a}) \in [p^k] \times R^{n-1}$ , columns indexed by  $x = (\tilde{x}, x_n) \in R^n$ , and entries

$$\mathbb{H}_{(m, \tilde{a}), x}^{(n)} = \phi_m(\langle \tilde{a}, \tilde{x} \rangle + x_n).$$

Let  $\tilde{a} = (a_1, \dots, a_{n-1}) \in R^{n-1}$  and  $m \in [p^k]$ . By (3.5) and then Proposition 6.2, we have

$$(7.4) \quad \begin{aligned} \phi_m(\langle \tilde{a}, \tilde{x} \rangle + x_n) &= \sum_{\ell_1 + \dots + \ell_{n-1} + \beta_n = m} \phi_{\ell_1}(a_1 x_1) \cdots \phi_{\ell_{n-1}}(a_{n-1} x_{n-1}) \phi_{\beta_n}(x_n) \\ &= \sum_{\ell_1 + \dots + \ell_{n-1} + \beta_n = m} \sum_{\tilde{\alpha}, \tilde{\beta}} \gamma(\tilde{\ell}, \tilde{\alpha}, \tilde{\beta}) \phi_{\tilde{\alpha}}(\tilde{a}) \phi_{\tilde{\beta}}(x), \end{aligned}$$

where we write

$$\begin{aligned} \tilde{\alpha} &= (\alpha_1, \dots, \alpha_{n-1}) \in [p^k]^{n-1}, \\ \beta &= (\tilde{\beta}, \beta_n) = (\beta_1, \dots, \beta_n) \in [p^k]^n, \\ \tilde{\ell} &= (\ell_1, \dots, \ell_{n-1}) \in [p^k]^{n-1}, \end{aligned}$$

and

$$(7.5) \quad \gamma(\tilde{\ell}, \tilde{\alpha}, \tilde{\beta}) = \prod_{j=1}^{n-1} c_{\ell_j, (\alpha_j, \beta_j)},$$

where  $c_{\ell_j, (\alpha_j, \beta_j)}$  are the coefficients in the expansion (6.2).

Let  $\Phi$  be the matrix with rows indexed by  $\beta \in [p^k]^n$ , columns indexed by  $x \in R^n$ , and entries  $\Phi_{\beta, x} = \phi_{\beta}(x)$ . Let also  $\Psi$  be the block-diagonal matrix with rows indexed by  $(m, \tilde{a}) \in [p^k]^n$ , columns indexed by  $(\mu, \tilde{\alpha}) \in R^n$ , and entries

$$\Psi_{(m, \tilde{a}), (\mu, \tilde{\alpha})} = \mathbf{1}_{m=\mu} \phi_{\tilde{\alpha}}(\tilde{a}).$$

Then (7.4) can be written in matrix form as

$$\mathbb{H}^{(n)} = \Psi \mathbb{B}^{(n)} \Phi,$$

where  $\mathbb{B}^{(n)}$  is the matrix with rows indexed by  $(m, \tilde{\alpha}) \in R^n$ , columns indexed by  $\beta \in [p^k]^n$ , and entries

$$\mathbb{B}_{(m, \tilde{\alpha}), \beta}^{(n)} = \sum_{\ell_1 + \dots + \ell_{n-1} + \beta_n = m} \gamma(\tilde{\ell}, \tilde{\alpha}, \tilde{\beta}).$$

Since both  $\Phi$  and  $\Psi$  are nonsingular by Lemma 5.1, it follows that  $\mathbb{H}^{(n)}$  and  $\mathbb{B}$  have the same rank. The next proposition completes the proof of Theorem 7.1.  $\square$

**Proposition 7.2.** *We have*

$$\text{rank}(\mathbb{B}^{(n)}) \leq 2 \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n}.$$

*Proof.* We claim that  $\mathbb{B}_{(m, \tilde{\alpha}), \beta}^{(n)} = 0$  for all  $m, \tilde{\alpha}, \beta$  such that

$$(7.6) \quad \sum_{j=1}^{n-1} \alpha_j + \sum_{j=1}^n \beta_j > m + 2(n-1)(p-1).$$

Indeed, assume that  $m, \tilde{\alpha}, \beta$  satisfy (7.6), and consider a contributing term

$$\gamma(\tilde{\ell}, \tilde{\alpha}, \tilde{\beta}) = \prod_{j=1}^{n-1} c_{\ell_j, (\alpha_j, \beta_j)} \text{ with } \ell_1 + \cdots + \ell_{n-1} + \beta_n = m.$$

By (7.6), we have

$$\sum_{j=1}^{n-1} (\alpha_j + \beta_j) + \beta_n > \sum_{j=1}^{n-1} \ell_j + \beta_n + 2(n-1)(p-1).$$

Hence there is at least one  $j$  such that  $\alpha_j + \beta_j > \ell_j + 2(p-1)$ . By Proposition 6.2, we have  $c_{\ell_j, (\alpha_j, \beta_j)} = 0$  for that  $j$ , so that  $\gamma(\tilde{\ell}, \tilde{\alpha}, \tilde{\beta}) = 0$ . Since this is true for all contributing terms, the claim follows.

Write  $|\tilde{\alpha}| = \sum_{j=1}^{n-1} \alpha_j$  and  $|\beta| = \sum_{j=1}^n \beta_j$  for short. We choose  $\lambda \in [p^k]$ , to be determined, and decompose  $\mathbb{B}^{(n)}$  into two matrices,  $\mathbb{B}_{\leq \lambda}^{(n)}$  and  $\mathbb{B}_{> \lambda}^{(n)}$ , with rows and columns indexed as for  $\mathbb{B}^{(n)}$ . Let  $\mathbb{B}_{\leq \lambda}^{(n)}$  be defined so that for any row indexed by  $(m, \tilde{\alpha})$  with  $m - |\tilde{\alpha}| \leq \lambda$ , the  $(m, \tilde{\alpha})$ -row of  $\mathbb{B}_{\leq \lambda}^{(n)}$  matches the  $(m, \tilde{\alpha})$ -row of  $\mathbb{B}^{(n)}$ . All other rows are zero. Then define  $\mathbb{B}_{> \lambda}^{(n)}$  so that

$$(7.7) \quad \mathbb{B}^{(n)} = \mathbb{B}_{\leq \lambda}^{(n)} + \mathbb{B}_{> \lambda}^{(n)}.$$

First consider  $\mathbb{B}_{\leq \lambda}^{(n)}$ . All its non-zero entries lie in rows indexed by  $(m, \tilde{\alpha})$  with  $m - |\tilde{\alpha}| \leq \lambda$ . By (7.6), any column indexed by  $\beta$  satisfying  $|\beta| > \lambda + 2(n-1)(p-1)$  is the zero vector. Thus bounding the rank of the matrix by its number of non-zero columns, we obtain

$$\begin{aligned} \text{rank}(\mathbb{B}_{\leq \lambda}^{(n)}) &\leq \#\{\beta \in [p^k]^n : |\beta| \leq \lambda + 2(n-1)(p-1)\} \\ &= \binom{\lambda + 2(n-1)(p-1) + n}{n} \end{aligned}$$

by Lemma 5.3.

Now we consider  $\mathbb{B}_{> \lambda}^{(n)}$ ; for this, we bound the rank of the matrix by its number of non-zero rows:

$$\begin{aligned} \text{rank}(\mathbb{B}_{> \lambda}^{(n)}) &\leq \#\{(m, \tilde{\alpha}) \in [p^k] \times [p^k]^{n-1} : m - |\tilde{\alpha}| > \lambda\} \\ &= \#\{(m, \tilde{\alpha}) \in [p^k] \times [p^k]^{n-1} : (p^k - 1 - m) + |\tilde{\alpha}| < p^k - 1 - \lambda\} \\ &= \binom{p^k - \lambda - 2 + n}{n} \end{aligned}$$

by Lemma 5.3 applied with  $\ell_1 = p^k - 1 - m$  and  $\ell_i = \alpha_i$  for  $i > 1$ .



Taking  $\lambda = \lfloor p^k/2 \rfloor - (n-1)(p-1)$ , and applying the subadditivity of rank to (7.7), we see that

$$\begin{aligned} \text{rank}(\mathbb{B}^{(n)}) &\leq \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n} + \binom{p^k - \lfloor p^k/2 \rfloor + (n-1)(p-1) - 2 + n}{n} \\ &\leq 2 \cdot \binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n}. \end{aligned}$$

□

## 8. GEOMETRIC TEST FOR HYPERPLANE FUNCTIONS

Theorem 7.1 shows that, in general, the linear span of affine hyperplane functions is strictly smaller than the span of phi functions of degree less than  $p^k$ . In this section we develop a geometric test for determining which phi functions are not in the span of hyperplane functions. In Subsection 8.2 we prove a specific case of the test in dimension  $n = 2$ , and then use it to show that a particular phi function is not in the span of hyperplane functions. Afterwards, we prove the test in generality. The full result is given in Theorem 8.3.

Recall that  $R = \mathbb{Z}/p^k\mathbb{Z}$ . To simplify the multiscale notation below, we will also write  $R_\ell = \mathbb{Z}/p^\ell\mathbb{Z}$  for  $1 \leq \ell \leq k$ , so that  $R_k = R$  and  $R_1 = \mathbb{Z}/p\mathbb{Z}$ . A *line* in a direction  $b \in R^n$  is a set of the form

$$L_b(a) = \{a + tb : t \in R\} \text{ for some } a \in R^n.$$

If  $b$  is nondegenerate,  $L_b(a)$  has  $|R| = p^k$  distinct elements.

In  $R^n$ , we define the *canonical directions* to be elements of the set  $\mathcal{B} = \bigcup_{i=1}^n \mathcal{B}_i$  where

$$\mathcal{B}_i = \{(p\ell_1, \dots, p\ell_{i-1}, 1, \ell_{i+1}, \dots, \ell_n) : \ell_i \in R\}.$$

Then any line  $L \subset R^n$  may be written in the form  $\{a + tb : t \in R\}$  for a unique direction vector  $b \in \mathcal{B}$ . Henceforth, when we refer to the direction of a line, this direction is an element of  $\mathcal{B}$ . For  $b, b' \in \mathcal{B}$ , we define the *p-adic angle* between  $b$  and  $b'$  to be  $\angle(b, b') = p^{-s}$  where  $p^s \parallel (b - b')$ . If  $L$  and  $L'$  are lines with directions  $b$  and  $b'$  respectively, we define the angle between them to be  $\angle(L, L') = \angle(b, b')$ .

For  $0 \leq \ell \leq k$ , define the projection map  $\pi_\ell : R^n \rightarrow R_\ell^n$  by

$$\pi_\ell(x) = x \bmod p^\ell.$$

Clearly, the mappings  $\pi_\ell$  are linear. For  $0 \leq \ell \leq k$ , define a *cube on scale  $\ell$*  to be a set of the form

$$Q = Q_\ell(x) = \{y \in R^n : \pi_\ell(y) = \pi_\ell(x)\} \subset R^n$$

for a fixed  $x \in R^n$ . In dimension  $n = 2$ , we refer to  $Q$  as a square. Note that a cube on scale 0 is the entire  $R^n$ , and a cube on scale  $k$  is a single point.

Next, we will define a type of set that we call a *fan*. Our geometric test will show that hyperplane functions are orthogonal to characteristic functions of fans.

**Definition 8.1. (Fans in dimension  $n = 2$ )** Let  $0 \leq \ell \leq p - 2$ . Let  $L_0, \dots, L_p$  be lines passing through a fixed cube  $Q$  on scale  $\ell + 1$  and satisfying  $\angle(L_i, L_j) = 1$  for each  $i \neq j$ . Let

$Q'$  be the cube on scale  $\ell$  containing  $Q$ . Then the set

$$X = \bigcup_{i=0}^p (L_i \cap Q') \setminus Q$$

is a fan on scale  $\ell$ .

For dimension  $n > 2$ , we will need a variant of the above configuration involving a  $(p+1)$ -tuple of lines in a neighbourhood of a 2-plane. We pause for a moment to define the relevant concepts. A 2-plane in  $R^n$  is the linear span over  $R$  of any two vectors  $u, v \in \mathcal{B}$  such that  $\angle(u, v) = 1$ . For a set  $S \subset R^n$ , and for  $j \in [k+1]$ , we define the  $p^{-j}$ -neighbourhood of  $S$  by

$$\mathcal{N}_j(S) = \{x \in R^k : \text{dist}(x, S) \leq p^{-j}\},$$

where we say that  $\text{dist}(x, S) = p^{-\ell}$  if  $\ell = \max\{j : p^j | (x - s) \text{ for some } s \in S\}$ .

**Definition 8.2. (Fans in dimension  $n > 2$ )** Let  $Q'$  be a cube on scale  $\ell$  in  $R^n$ . Define

$$\Pi := Q' \cap \mathcal{N}_{\ell+1}(\Pi_0),$$

where  $\Pi_0$  is a 2-plane passing through some point  $a \in Q'$ . Let  $Q = Q_{\ell+1}(a) \subset Q' \cap \Pi$  be the cube on scale  $\ell+1$  containing  $a$ . Let  $L_0, \dots, L_p \subset R^n$  be lines that pass through  $Q$ , make pairwise angles 1, and such that  $L_j \cap Q' \subset \Pi$  for each  $j$ . Then

$$X = \bigcup_{i=0}^p (L_i \cap Q') \setminus Q$$

is a fan on scale  $\ell$ .

**Theorem 8.3.** Let  $f \in \mathcal{H}^n$  be a hyperplane function, and let  $X \subset R^n$  be a fan. Then

$$\sum_{x \in R^n} f(x) \mathbf{1}_X(x) = 0 \pmod{p}.$$

To prove the theorem, it suffices to prove that  $|H \cap X| = 0 \pmod{p}$  for any hyperplane  $H$  and any fan  $X$ . We prove this in Proposition 8.11.

**8.1. Preliminary lemmas.** Let  $Q$  be a cube on scale  $\ell$ . For  $x \in Q$ , write  $x = x' + p^\ell x''$  with  $x' \in [p^\ell]$  and  $x'' \in [p^{k-\ell}]$ . Note that if  $x, y \in Q$ , then (with the obvious notation) we have  $y' = x'$ . We may therefore identify  $Q$  with  $R_{k-\ell}^n$  via the map  $\iota_Q : Q \rightarrow R_{k-\ell}^n$  defined by

$$\iota_Q(x' + p^\ell x'') = x''.$$

**Lemma 8.4. (Properties of  $\iota_Q$ )** Let  $Q$  be a cube on scale  $\ell$  for some  $0 \leq \ell \leq k-1$ . Then:

- (i) If  $L \subset R^n$  is a line in direction  $b$  intersecting  $Q$ , then  $\iota_Q(Q \cap L)$  is a line in direction  $\pi_{k-\ell}(b)$  in  $R_{k-\ell}^n$ .
- (ii) If  $H \subset R^n$  is a hyperplane with normal direction  $b$  intersecting  $Q$ , then  $\iota_Q(Q \cap H)$  is a hyperplane with normal direction  $\pi_{k-\ell}(b)$  in  $R_{k-\ell}^n$ .
- (iii) If  $\Pi \subset R^n$  is a 2-plane intersecting  $Q$ , then  $\iota_Q(\Pi)$  is a 2-plane in  $R_{k-\ell}^n$ .
- (iv) If  $S \subset Q$ , and if  $j \geq \ell$ , then  $\iota_Q(\mathcal{N}_j(S)) = \mathcal{N}_{j-\ell}(\iota_Q(S))$ .

*Proof.* Pick some point  $a \in Q \cap L$ , and suppose  $a = a' + p^\ell a''$  with  $a' \in [p^\ell]$ . Then

$$Q \cap L = \{a + (\lambda p^\ell)b : \lambda \in R_{k-\ell}\},$$

and so

$$\iota_Q(Q \cap L) = \{a'' + \lambda \pi_{k-\ell}(b) : \lambda \in R_{k-\ell}\} \subset R_{k-\ell}^n.$$

Now suppose  $H = \{x : \langle x - c, b \rangle = 0\}$ , and  $a \in H \cap Q$ . Then

$$Q \cap H = \{a + y : y = p^\ell y'', \langle y, b \rangle = 0 \pmod{p^k}\} = \{a + p^\ell y'' : \langle y'', b \rangle = 0 \pmod{p^{k-\ell}}\}$$

and so

$$\iota_Q(Q \cap H) = \{a'' + y'' : \langle y'', \pi_{k-\ell}(b) \rangle = 0\} \subset R_{k-\ell}^n.$$

The proof of (iii) is similar. Finally, (iv) follows from the observation that for  $x, y \in Q$  and for  $i \geq \ell$ ,

$$p^i \mid (x - y) \quad \text{if and only if} \quad p^{i-\ell} \mid (\iota_Q(x) - \iota_Q(y)).$$

□

**Lemma 8.5. (Properties of  $\pi_\ell$ )** For  $0 \leq \ell \leq k - 1$ , the following statements hold:

- (i) If  $L \subset R^n$  is a line in direction  $b$ , then  $\pi_\ell(L) \subset R_\ell^n$  is a line in direction  $\pi_\ell(b)$ . In particular, if  $\angle(L, L') = 1$  in  $R^n$ , then  $\angle(\pi_\ell(L), \pi_\ell(L')) = 1$  in  $R_\ell^n$ .
- (ii) If  $H \subset R^n$  is a hyperplane with normal direction  $b$ , then  $\pi_\ell(H) \subset R_\ell^n$  is a hyperplane with normal direction  $\pi_\ell(b)$ .
- (iii) If  $\Pi \subset R^n$  is a 2-plane spanned by  $b, b' \in \mathcal{B}$ , then  $\pi_\ell(\Pi) \subset R_\ell^n$  is a 2-plane spanned by  $\pi_\ell(b), \pi_\ell(b')$ .
- (iv) If  $S \subset R^n$ , and if  $j \geq \ell$ , then  $\pi_\ell(\mathcal{N}_j(S)) = \pi_\ell(S)$ .

*Proof.* By linearity, if  $L = \{a + tb : t \in R\}$  is a line, then

$$\pi_\ell(L) = \{\pi_\ell(a) + t' \pi_\ell(b) : t' \in R_\ell\}.$$

This proves (i). For (ii), suppose  $H = \{x : \langle x - a, b \rangle = 0\}$ . We claim that

$$(8.1) \quad \pi_\ell(H) = \{x' \in R_\ell : \langle x' - a', b' \rangle = 0\}.$$

Indeed, writing  $x = x' + x'' p^\ell$ , and similarly for  $a$  and  $b$ , we have

$$\langle x - a, b \rangle = \langle x' - a', b' \rangle + p^\ell (\langle x' - a', b'' \rangle) + \langle x'' - a'', b \rangle.$$

Applying  $\pi_\ell$  to both sides of this equation, and noting that  $\pi_\ell(0) = 0$ , we conclude that  $\pi_\ell(H) \subset \{x' \in R_\ell : \langle x' - a', b' \rangle = 0\}$ . Conversely, suppose  $x' \in [p^\ell]$  satisfies  $\langle x' - a', b' \rangle = 0 \pmod{p^\ell}$ . Then for any  $x''$  satisfying

$$\langle x' - a', b'' \rangle + \langle x'' - a'', b \rangle = 0 \pmod{p^{k-\ell}},$$

we have  $x = x' + x'' p^\ell \in H$  (notice that such an  $x''$  must exist as  $b$  is non-zero mod  $p$ ). This gives (8.1) The proof of (iii) is similar. Finally, (iv) follows directly from the definitions of the  $p^{-j}$  neighbourhood of a set and the map  $\pi_\ell$ . □

**Lemma 8.6.** Let  $L, L' \subset R^n$  be lines. Assume that  $\angle(L, L') = 1$ , and that  $L$  and  $L'$  both intersect a cube  $Q$  on scale 1. Then  $L \cap L' \subset Q$ .

*Proof.* Suppose  $L$  and  $L'$  intersect in some cube  $Q'$  on scale 1. Then the lines  $\pi_1(L)$  and  $\pi_1(L')$  in  $R_1^n$  pass through both of the points  $q' = \pi(Q')$  and  $q = \pi(Q)$ . But Lemma 8.5 implies that  $\pi_1(L)$  and  $\pi_1(L')$  make angle 1, hence intersect uniquely. Therefore  $q = q'$ , which means that  $Q = Q'$ , and indeed any intersection points of  $L$  and  $L'$  lie in  $Q$ . □

**Lemma 8.7.** *Let  $L \subset R^n$  be a line in direction  $b$ , and let  $H \subset R^n$  be a hyperplane with normal direction  $v$ . Assume that they intersect, and that  $\langle b, v \rangle = cp^j$  for some invertible  $c \in R^\times$  and  $j \geq 0$ . If  $j = 0$ , then the intersection point is unique. If  $j > 0$ , then there is some cube  $Q$  on scale  $k - j$  so that  $L \cap H \subset Q$ , and  $|L \cap H| = p^j$ .*

*Proof.* Let  $a \in L \cap H$ , so that  $L = \{a + tb : t \in R^n\}$  and  $H = \{x : \langle x - a, v \rangle = 0\}$ . Then  $L \cap H$  consists of points  $x = a + tb$  with  $t \in R$  such that

$$0 = \langle x - a, v \rangle = t \langle b, v \rangle = tcp^j \pmod{p^k}.$$

If  $j = 0$ , then we have a unique intersection point with  $t = 0$ . If  $j \geq 1$ , the intersection points correspond to  $t = 0 \pmod{p^{k-j}}$ , that is,  $t = \ell p^{k-j}$  for  $\ell \in [p^j]$ . This yields  $p^j$  intersection points, all in the same cube on scale  $k - j$ .  $\square$

**8.2. A simplified geometric test.** In this subsection we prove Theorem 8.3 in the simple case when  $n = 2$  and  $\ell = 0$ ; the general case is deferred until the next subsection.

Let  $\mathcal{L} = \{L_0, L_1, \dots, L_p\}$  be a collection of  $p + 1$  lines in  $R^2$ . Assume that there is some square  $Q$  on scale 1 such that  $Q \cap L_i \neq \emptyset$  for all  $i$ , and that  $\angle(L_i, L_j) = 1$  for any  $i \neq j$ . Notice that, if  $B$  is the set of directions of the lines  $L_i$ , then

$$(8.2) \quad \{b \pmod{p} : b \in B\} = \{(0, 1), (1, 0), (1, 1), \dots, (1, p - 1)\}.$$

If  $L$  is any line in  $R^2$ , then there is a unique line  $L_i$  in  $\mathcal{L}$  such that  $\angle(L, L_i) < 1$ .

**Lemma 8.8.** *Let  $L, L'$  be lines in  $R^2$ . Let  $b$  be the direction of  $L$ , and  $v$  the normal direction of  $L'$ .*

(i) *If  $\angle(L, L') = 1$ , then  $\langle v, b \rangle \neq 0 \pmod{p}$ . Consequently, by Lemma 8.7,  $L$  and  $L'$  have a unique intersection point.*

(ii) *If  $\angle(L, L') < 1$ , then  $\langle v, b \rangle = 0 \pmod{p}$ . Consequently, by Lemma 8.7, for any square  $Q$  on scale 1 we have  $|L \cap L' \cap Q| = 0 \pmod{p}$ .*

*Proof.* For any  $b, v \in \mathcal{B}$ , the directions  $b$  and  $v \pmod{p}$  must belong to the set on the right side of (8.2). The lemma is now easy to verify directly.  $\square$

**Proposition 8.9.** *Let  $\mathcal{L}$  and  $Q$  be as described above. Let*

$$X = \bigcup_{i=0}^p L_i \setminus Q.$$

*Then for any line  $L$ , we have  $|L \cap X| = 0 \pmod{p}$ .*

*Proof.* Let  $L$  be a line. By the observation in (8.2), there is a unique line  $L'$  in  $\mathcal{L}$  such that  $\angle(L, L') < 1$ . Without loss of generality, assume  $L' = L_0$ .

Notice that for  $i \neq j$ , the intersection of  $L_i$  and  $L_j$  is contained in  $Q$ , by Lemma 8.6. Therefore no two distinct lines in  $\mathcal{L}$  may intersect in  $X$ , so that

$$(8.3) \quad |L \cap X| = \sum_{i=0}^p |L \cap L_i \cap X|.$$

First suppose that  $L \cap Q = \emptyset$ . Then by Lemma 8.8, for each  $i \in \{1, \dots, p\}$ ,  $L$  intersects  $L_i$  at a unique point  $p_i \notin Q$ , so  $|L \cap L_i \cap X| = 1$  for  $i = 1, \dots, p$ . Next we count the size of  $L \cap L_0 \cap X$ . By Lemma 8.8, the size of  $L \cap L_0$  in any square of scale 1 is 0 modulo  $p$ , so

$|L \cap L_0 \cap X| = 0 \pmod p$ . Combining this all with (8.3), we obtain  $|L \cap X| = 0 \pmod p$ , as desired.

Now suppose  $L \cap Q \neq \emptyset$ . Then by Lemma 8.6, for  $i = 1, \dots, p$ , we have that  $L \cap L_i \subset Q$ , and so  $L \cap L_i \cap X = \emptyset$ . Therefore  $X \cap L = X \cap L \cap L_0$ , and by the same argument as in the previous case, the size of this set is 0 modulo  $p$ .  $\square$

*Example.* We can use the previous proposition to show that in  $(\mathbb{Z}/4\mathbb{Z})^2$ , the phi function  $\phi_{21}$  does not lie in the span of hyperplane functions. We record the values of  $\phi_{21}(x, y)$  in the following table, with rows indexed by  $y \in \mathbb{Z}/4\mathbb{Z}$  and columns by  $x \in \mathbb{Z}/4\mathbb{Z}$ :

	0	2	1	3
0	0	0	0	0
2	0	0	0	0
1	0	1	0	1
3	0	1	0	1

We used dashed lines in the table to partition  $(\mathbb{Z}/4\mathbb{Z})^2$  according to its four squares on scale 1. Let  $Y = \text{supp } \phi_{21}$ . Observe that  $\pi_1(Y) = \{(0, 1), (1, 1)\} \subset (\mathbb{Z}/2\mathbb{Z})^2$  is a line in the direction  $(1, 0)$ , whereas for each square  $Q$  on scale 1, the set  $\iota_Q(Y \cap Q)$  is either empty or else a line in the direction  $(0, 1)$ . In this sense,  $Y$  is a line both globally on the rough scale and locally on each square on scale 1, but the directions on the two scales are inconsistent with each other.

One could ask if there might be a way to represent  $\phi_{21}$  as a linear combination of several hyperplane functions. Our geometric test shows that this is in fact impossible. Take  $Q$  to be the square containing the point  $(0, 1)$ . Let  $L_0, L_1, L_2$  be lines in directions  $(1, 0)$ ,  $(1, 1)$ , and  $(0, 1)$ , respectively, all passing through the point  $(0, 1)$ . Let  $X = (L_0 \cup L_1 \cup L_2) \setminus Q$ . Then  $X \cap Y = \{(3, 1)\}$ , and so

$$\sum_{(x,y) \in X} \phi_{21}(x, y) = 1 \neq 0 \pmod 2.$$

**8.3. Generalizing the geometric test.** Let  $n > 2$  and let  $\Pi \subset R^n$  be a  $p^{-1}$ -neighbourhood of a 2-plane in  $R^n$ . For our hyperplane test in  $R^n$ , we will consider the intersection of a hyperplane  $H$  with  $\Pi$ , and then apply an adapted form of the 2-dimensional hyperplane test in  $\Pi$ . The details in the case  $\ell = 0$  are given in the following proposition.

**Proposition 8.10.** *Let  $\Pi \subset R^n$  be as defined above, and let  $Q$  be a cube on scale 1 in  $\Pi$ . Let  $L_0, L_1, \dots, L_p \subset \Pi$  be lines in  $R^n$  all passing through  $Q$  and satisfying  $\angle(L_i, L_j) = 1$  for all  $i \neq j$ . Let  $X = (\bigcup_{j=0}^p L_j) \setminus Q$ . If  $H \subset R^n$  is a hyperplane, then  $|X \cap H| = 0 \pmod p$ .*

*Proof.* Observe that by Lemma 8.6, the lines  $L_j$  may only intersect in  $Q \subset X^c$ , and so

$$(8.4) \quad |X \cap H| = \sum_{j=0}^p |X \cap L_j \cap H|.$$

Let  $b$  be the normal direction of  $H$  and  $b^{(j)}$  the direction of  $L_j$ . By Lemma 8.5,  $\pi_1(\Pi)$  is a 2-plane in  $R_1^n$  and  $\pi_1(H)$  is a hyperplane in  $R_1^n$  with normal direction  $\pi_1(b)$ . Then either  $\pi_1(\Pi) \subset \pi_1(H)$ , or else  $\pi_1(\Pi) \cap \pi_1(H)$  is a line. In the first case,  $\pi_1(L_j) \subset \pi_1(H)$ , so that

$\langle b^{(j)}, b \rangle = 0 \pmod p$  for all  $j$ . By Lemma 8.7, for each  $j$  and in each cube  $Q'$  on scale 1, we have  $|H \cap L_j \cap Q'| = 0 \pmod p$ , which together with (8.4) gives the desired result.

Thus for the remainder of the proof we assume that  $\bar{L} := \pi_1(H) \cap \pi_1(\Pi)$  is a line, and also that there is some  $j$  so that  $|X \cap L_j \cap H| \neq 0 \pmod p$  (as otherwise, (8.4) gives the desired result), in which case Lemma 8.7 implies that the size of the intersection is 1. For  $i \in [p+1]$ , let  $\bar{L}_i = \pi_1(L_i)$ . By Lemma 8.5,  $\bar{L}_0, \bar{L}_1, \dots, \bar{L}_p$  are lines so that any pair makes angle 1, and all pass through the point  $q = \pi_1(Q)$ . Moreover, each is contained in the 2-plane  $\pi_1(\Pi)$ , and so they inherit properties of lines in  $R_1^2$ .

Thus  $\bar{L}$  has the same direction as exactly one of the  $\bar{L}_i$ , and intersects the other  $p$  lines uniquely. Without loss of generality, assume  $\bar{L}$  is parallel to  $\bar{L}_0$ . Since  $H$  intersects  $L_j$  outside of  $Q$ , the unique intersection of  $\bar{L}_j$  and  $\bar{L}$  is not equal to the point  $q$ , and in particular,  $q \notin \bar{L}$ . Thus  $\bar{L}_0 \cap \bar{L}$  is empty, and so  $L_0 \cap H$  is empty as well. Moreover,

$$(8.5) \quad |\bar{L}_i \cap \bar{L}| = |(\bar{L}_i \cap \bar{L}) \setminus \{q\}| = 1 \quad \text{for each } i = 1, \dots, p,$$

since  $\bar{L}_i$  and  $\bar{L}$  intersect uniquely, and the latter line does not intersect  $q$ . Also for such  $i$ , let

$$Q_i = \pi_1^{-1}(\bar{L} \cap \bar{L}_i).$$

Then  $Q_i$  is a cube on scale 1 in  $\Pi$  that contains  $X \cap L_i \cap H = L_i \cap H$ . Combining this with (8.4), we have

$$|X \cap H| = \sum_{i=1}^p |L_i \cap H| = \sum_{i=1}^p |(L_i \cap Q_i) \cap (H \cap Q_i)|.$$

We will show that  $|(L_i \cap Q_i) \cap (H \cap Q_i)| = 1$  for  $i = 1, \dots, p$ , which will complete the proof. To this end, choose  $i \in \{1, \dots, p\}$ , and identify  $Q_i$  with  $R_{k-1}^n$  via the map  $\iota_{Q_i}$ . Since this map is a bijection, we prove  $|\iota_{Q_i}(L_i) \cap \iota_{Q_i}(H)| = 1$ .

By Lemmas 8.4 and 8.5, if  $v$  is the direction of  $\iota_{Q_i}(L_i)$ , then  $\pi_1(v)$  is the direction of  $\bar{L}_i$ , and if  $b$  is the normal direction of  $\iota_{Q_i}(H)$ , then  $\pi_1(b)$  is the normal direction of  $\pi_1(H)$ . Since  $\bar{L}_i$  is contained in  $\pi_1(\Pi)$ , we have

$$\bar{L}_i \cap \pi_1(H) = \bar{L}_i \cap \pi_1(\Pi) \cap \pi_1(H) = \bar{L}_i \cap \bar{L}.$$

By (8.5), the last intersection is a single point in  $R_1^n$ . It follows by Lemma 8.7 that  $\langle \pi_1(b), \pi_1(v) \rangle \neq 0 \pmod p$ . But then  $\langle b, v \rangle \neq 0 \pmod p$ , and so the same lemma gives that  $\iota_{Q_i}(L_i)$  and  $\iota_{Q_i}(H)$  intersect uniquely as well.  $\square$

Now we generalize this argument, and the argument for  $n = 2$ , to cubes on other scales.

**Proposition 8.11.** *Let  $n \geq 2$ . For any hyperplane  $H \subset R^n$  and any fan  $X \subset R^n$ , we have  $|H \cap X| = 0 \pmod p$ .*

*Proof.* First assume  $n > 2$ . Let  $X = \bigcup_{i=0}^p (L_i \cap Q') \setminus Q$  be a fan as in Definition 8.2. By Lemma 8.4,  $\iota_{Q'}(L_0), \dots, \iota_{Q'}(L_p)$  are lines so that each pair makes a  $p$ -adic angle 1, and  $\iota_{Q'}(H)$  is a hyperplane. Moreover,  $\iota_{Q'}(L_0), \dots, \iota_{Q'}(L_p)$  are all contained in  $\iota_{Q'}(\Pi)$ , and each passes through  $\iota(Q)$ , a cube in  $R_{k-\ell}^n$  on scale 1. By Lemma 8.4 (iii) and (iv),  $\iota_{Q'}(\Pi)$  is the  $p^{-1}$ -neighbourhood of a 2-plane in  $R_{k-\ell}^n$ . We may now apply Proposition 8.10 to conclude  $|\iota_{Q'}(H) \cap \iota_{Q'}(X)| = 0 \pmod p$ . Since  $\iota_{Q'}$  is a bijection, we have  $|H \cap X| = 0 \pmod p$ .

The  $n = 2$  case is similar, although we apply Proposition 8.9 instead.  $\square$

8.4. **Parallel lines.** Any hyperplane  $H$  in  $R^n$  has the following property. Let  $Q$  is a cube on some scale  $\ell$ , and let  $L, L'$  be two parallel lines in  $R^n$ , both passing through  $Q$ . Then

$$|L \cap Q \cap H| \equiv |L' \cap Q \cap H| \pmod{p}.$$

We prove in Proposition 8.12 that a similar property holds for phi functions.

**Proposition 8.12.** *Let  $Q$  be a cube on scale  $\ell$  for some  $0 \leq \ell \leq k - 1$ . Let  $L, L'$  be two lines in  $R^n$  in the direction of the same vector  $b \in \mathbb{P}R^{n-1}$ , and assume that both  $L$  and  $L'$  pass through  $Q$ . Then for any function  $f \in \Omega_{p^{k-1}}^n$  we have*

$$\langle \mathbf{1}_{L \cap Q}, f \rangle \equiv \langle \mathbf{1}_{L' \cap Q}, f \rangle \pmod{p}.$$

*Proof.* We prove the proposition under the assumption that  $Q = R^n$ . The general case can be deduced from this by rescaling as in the proof of Proposition 8.11. The details are left to the interested reader.

We first claim that it suffices to consider the case when  $L, L'$  are lines in the direction of  $e_1 = (1, 0, \dots, 0)$ . Indeed, let  $b \in \mathbb{P}R^{n-1}$  be the common direction vector for  $L$  and  $L'$ . Without loss of generality, we may assume that  $b_1 \in R^\times$ . Define a linear mapping  $U : R^n \rightarrow R^n$  by saying that  $U(e_1) = b$  and (with the obvious notation)  $U(e_j) = e_j$  for  $2 \leq j \leq n$ . In the basis  $e_1, \dots, e_n$ ,  $U$  is represented by the matrix

$$\begin{pmatrix} b_1 & 0 & 0 & \cdots & 0 \\ b_2 & 1 & 0 & \cdots & 0 \\ b_3 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ b_n & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Since the determinant of this matrix is  $b_1 \in R^\times$ ,  $U$  is invertible. Moreover,  $U^{-1}$  maps lines in the direction of  $b$  to lines in the direction of  $e_1$ . By iterated applications of (3.5) and Lemma 4.7,  $f(x)$  and  $f(Ux)$  have the same degree. This proves the claim.

It therefore suffices to prove the following: if  $L, L'$  are lines in the direction of  $e_1$ , then for any  $\alpha$  with  $|\alpha| \leq p^k - 1$  we have

$$(8.6) \quad \langle \mathbf{1}_L, \phi_\alpha \rangle \equiv \langle \mathbf{1}_{L'}, \phi_\alpha \rangle \pmod{p}.$$

Let  $L$  be the line  $\{(y, z) : y \in R\}$  for some  $z \in R^{n-1}$ . Let also  $\alpha = (\beta, \gamma)$  with  $\beta \in [p^k]$  and  $\gamma \in [p^k]^{n-1}$ . Then

$$\begin{aligned} \langle \mathbf{1}_L, \phi_\alpha \rangle &= \sum_{y \in R} \phi_\beta(y) \phi_\gamma(z) \\ &= \phi_\gamma(z) \sum_{y \in R} \prod_{j=0}^{k-1} \phi_{\beta_j}(y_j) \\ &= \phi_\gamma(z) \prod_{j=0}^{k-1} \left( \sum_{y_j=0}^{p-1} \phi_{\beta_j}(y_j) \right), \end{aligned}$$

where  $y = \sum y_j p^j$  and  $\beta = \sum \beta_j p^j$  are the  $p$ -adic expansions of  $y$  and  $\beta$ .

If  $0 \leq \beta_j < p - 1$  for some  $j$ , then by (3.3),

$$(8.7) \quad \sum_{y_j=0}^{p-1} \phi_{\beta_j}(y_j) = \sum_{y_j=0}^{p-1} (\phi_{\beta_j+1}(y_j + 1) - \phi_{\beta_j+1}(y_j)) = 0.$$

If both of the expressions  $\langle \mathbf{1}_L, \phi_\alpha \rangle$  and  $\langle \mathbf{1}_{L'}, \phi_\alpha \rangle$  are zero mod  $p$ , then (8.6) is clearly true. On the other hand, if either expression is nonzero mod  $p$ , it follows from (8.7) that  $\beta_j = p - 1$  for all  $j$ . But then  $\beta = p^k - 1$ . Since  $\beta + |\gamma| = |\alpha| \leq p^k - 1$ , it follows that  $|\gamma| = 0$ , so that  $\phi_\gamma(z) = 1$ . But then  $\phi_\alpha$  is the characteristic function of the hyperplane  $x_1 = p^k - 1$ , and (8.6) is again true with both sides equal to 1. This proves the proposition.  $\square$

## 9. ACKNOWLEDGEMENT

The first author was supported by NSERC Discovery Grant 22R80520. The second author was supported by NSERC Discovery Grants 22R80520 and GR010263.

## REFERENCES

1. B. Arsovski, *The  $p$ -adic Kakeya conjecture*, J. Amer. Math. Soc. 37 (2024), 69–80.
2. J. Blasiak, T. Church, H. Cohn, J. A. Grochow, E. Naslund, W. F. Sawin, and C. Umans, *On cap sets and the group-theoretic approach to matrix multiplication*, Discrete Analysis 2017:3, 27 pp.
3. M. Dhar, *The Kakeya set conjecture over  $\mathbb{Z}/N\mathbb{Z}$  for general  $N$* , arXiv:2110.14889, to appear in Advances in Combinatorics.
4. M. Dhar, *Maximal and  $(m, \epsilon)$ -Kakeya bounds over  $\mathbb{Z}/N\mathbb{Z}$  for general  $N$* , preprint, 2022, arXiv:2209.11443
5. M. Dhar,  *$(n, k)$ -Besicovitch sets do not exist in  $\mathbb{Z}_p^n$  and  $\hat{\mathbb{Z}}^n$  for  $k \geq 2$* , preprint, 2023, arXiv:2312.02495
6. M. Dhar, Z. Dvir, *Proof of the Kakeya set conjecture over rings of integers modulo square-free  $N$* , Combinatorial Theory 1(2021), # 4, 21pp.
7. Z. Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. 22 (2009), 1093–1097.
8. Z. Dvir, P. Gopalan, S. Yekhanin, *Matching Vector codes*, SIAM Journal on Computing, 40(4) (2011), 1154–1178.
9. Z. Dvir, G. Hu, *Matching-Vector families and LDCs over large modulo*. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 513–526. Springer, 2013.
10. J. S. Ellenberg, D. Gijswijt, *On large subsets of  $\mathbb{F}_q^n$  with no three-term arithmetic progression*, Annals of Math, 185(1) (2017), 339–343.
11. J. M. Goethals, P. Delsarte, *On a class of majority-logic decodable cyclic codes*, IEEE Transactions on Information Theory, 14(2) (1968), 182–188.
12. J. Hickman, J. Wright, *The Fourier restriction and Kakeya problems over rings of integers modulo  $N$* , Discrete Analysis 2018:11, 54 pp.
13. A. Leibman, *Polynomial mappings of groups*. Israel J. Math. 129:29–60 (2002).
14. F. J. MacWilliams, H. B. Mann, *On the  $p$ -rank of the design matrix of a difference set*, Inf. Control., 12:474–488, 1968.
15. F. Petrov. *Combinatorial results implied by many zero divisors in a group ring*, preprint, 2016, arXiv:1606.03256.
16. K.J.C. Smith, *On the  $p$ -Rank of the Incidence Matrix of Points and Hyperplanes in a Finite Projective Geometry*, J. Comb. Theory 7 (1969), 122–129.
17. D. Speyer, *Bounds for sum free sets in prime power cyclic groups — three ways*, blog post at <https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-in-prime-power-cyclic-groups-three-ways/>
18. C. Yuan, Q. Guo, H. Kan, *A novel elementary construction of matching vectors*, Information Processing Letters, 112(12) (2012), 494–496.



DEPARTMENT OF MATHEMATICS, UBC, VANCOUVER, B.C. V6T 1Z2, CANADA  
*ilaba@math.ubc.ca, ctrainor@math.ubc.ca*