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

Izabella Łaba*[1] and Charlotte Trainor†[2]

[1]*Department of Mathematics, UBC, Vancouver, B.C. V6T 1Z2, Canada*
ilaba@math.ubc.ca
[2]*Department of Mathematics, UBC, Vancouver, B.C. V6T 1Z2, Canada*
Current address: Department of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A.
trainor@math.harvard.edu

Submitted: Mar 25, 2024; Accepted: Dec 10, 2024; Published: Mar 15, 2025

Abstract. For p prime, let $\mathcal{H}^n$ be the linear span of indicator 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 $\mathcal{H}^n$.

Keywords. Hyperplanes, generalized polynomials, binomial coefficients

Mathematics Subject Classifications. 05B20, 05B25, 05A10

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 $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$.

Recall that the projective space $\mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}$ is the quotient space $((\mathbb{Z}/p\mathbb{Z})^n \setminus \{0\})/\sim$, where $\sim$ is the equivalence relation

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

*Supported by NSERC Discovery Grant 22R80520.
†Supported by NSERC Discovery Grants 22R80520 and GR010263.

When $k > 1$, the projective space over R^n must be defined a little bit more carefully. Let $R^{n,\times}$ be the set of all elements of R^n that have at least one invertible component. We then define

$$\mathbb{P}R^{n-1} = R^{n,\times}/R^\times.$$

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

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

This is how directions in R^n are often defined in the literature, see e.g. [HW18]. All directions will be assumed to be nondegenerate unless explicitly stated otherwise.

A (nondegenerate) *hyperplane* is a set of the form

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

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*.

By convention, we will refer to nondegenerate hyperplanes as simply hyperplanes; whenever we work with degenerate hyperplanes (as in Definition 1.1 (i) below), we will say so explicitly. 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 linear space of functions from R^n to $\mathbb{Z}/p\mathbb{Z}$. We will refer to the elements of $\mathcal{H}^n$ as *hyperplane functions*.

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 indexed by $b \in R^n$ and columns indexed by $x \in R^n$, such that

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

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

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

(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

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

Note that the equation $\langle b, x\rangle = 0$ in (i) does not define a hyperplane in our sense if b is not a nondegenerate direction; however, we use the terminology above for consistency with the existing literature such as [DD21].

We are interested in upper and lower bounds on the rank of these matrices over $\mathbb{Z}/p\mathbb{Z}$. This also provides bounds on the dimension of $\mathcal{H}^n$, since we have directly from the definition

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{H}^n) = \operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}^*_{p^k,n}).$$

For $k = 1$, the rank of $W_{p,n}$ is known as a special case of the results in [GD68, MM68, Smi69].

Theorem 1.2 ([GD68, MM68, Smi69])**.** *For p prime and $n \in \mathbb{N}$,*

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

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 the space of all polynomial functions on $\mathbb{F}_p^n$ of total degree at most $p-1$. Moreover, the subspace $\mathcal{H}_0^n$ spanned by homogeneous hyperplanes is identical to the linear span of all homogeneous polynomial functions of degree exactly $p-1$, together with the constant function. Counting such polynomials produces the bound in Theorem 1.2. We provide the full argument in Section 5.2.

Our interest in hyperplane functions for $k \geqslant 2$ is motivated in part by the work of Dhar and Dvir [DD21], where a connection was established 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 lower bound [Dvi09] on the size of Kakeya sets in $(\mathbb{Z}/p\mathbb{Z})^n$, and then extended their argument to prove the Kakeya conjecture in $(\mathbb{Z}/N\mathbb{Z})^n$ for squarefree N.

For $k \geqslant 2$, Dhar and Dvir were still able to bound[1] the size of Kakeya sets in R^n from below by the $\mathbb{F}_p$-rank of $W^*_{p^k,n}$. Unfortunately, hyperplane functions in R^n with $k \geqslant 2$ are less well understood. Dhar and Dvir [DD21, Lemma 5.3] observed 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 [DGY11, YGK12] yields a lower bound on the rank of $W_{p^k,n}$ of the order $p^{kn/2}$, which is not sufficient for good lower bounds on Kakeya sets.

On the other hand, the rank of $W^*_{p^k,n}$ is trivially bounded from above by the number of directions in $\mathbb{P}R^{n-1}$, therefore by the number of vectors in R^n with at least one coordinate equal to 1, which we may bound from above by $np^{k(n-1)}$. Together with the easy estimate in Proposition 2.2 below, this yields the bound

$$\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n}) \leqslant 1 + knp^{k(n-1)}. \tag{1.2}$$

The Kakeya conjecture in R^n was eventually resolved by Arsovski [Ars24], based on a comparison of the size of Kakeya sets to the rank of a related but different matrix $M_{p^k,n}$ (we define it in (2.14)). Subsequently, Dhar [Dha24] proved the Kakeya conjecture in $\mathbb{Z}/N\mathbb{Z}$ for general N,

[1] In [DD21, Theorem 1.6], the authors refer to the rank of $W_{p^k,n}$, but their proof 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.

with further progress in [Dha22, Dha23b]. In [Dha23a, Lemma 2.2.14], Dhar used a modification of Arsovski's method to prove that

$$\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n}) \geqslant \binom{\lceil p^k/k \rceil + n - 1}{n-1}. \tag{1.3}$$

Dhar also noted an upper bound on $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n})$ that can be obtained by similar methods; however, that bound has the order of magnitude p^{kn}, which is weaker than (1.2). We provide the details in Section 2.2.

We are interested in obtaining upper bounds on $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(W_{p^k,n})$ that come closer to (1.3). For $k \geqslant 2$, the conventional polynomial method is less feasible than for $k = 1$, basically because there are not sufficiently many polynomial functions to span all hyperplane functions. When working modulo p as we do here, any polynomial function from R to $\mathbb{Z}/p\mathbb{Z}$ can be represented by a polynomial of degree at most $p-1$ in each variable by Fermat's Little Theorem. Working modulo p^k instead would not fix the problem: since the polynomial $(x^p - x)^k$ is null mod p^k, any polynomial function $R \to R$ can be represented by a polynomial of degree $O(kp)$ in each variable (see also [Kem21, Li05, Wil06] for a more detailed analysis). We remedy this by using binomial coefficients as generalized polynomial functions from R to $\mathbb{Z}/p\mathbb{Z}$. This allows us to define generalized polynomials of degree up to $p^k - 1$, which is sufficient to span $\mathcal{H}^n$.

It is well known (going back at least to the work of Fréchet [Fré09]) that polynomial functions admit a characterization based on the calculus of finite differences. This gave rise to broad generalizations of the concept of polynomial functions to settings where polynomials in the classic sense might not be well defined. General frameworks for polynomial functions on groups were developed and used by various authors, including Leibman [Lei02], Laczkovich [Lac04], Aichinger and Moosbauer [AM21], Clark and Schauz [CS22, CS23].

Binomial coefficients are a natural choice of generalized polynomials, thanks to Pascal's identity which regulates their behaviour under discrete derivatives. A systematic treatment of binomial coefficients from this point of view was given by Schauz [Sch14] (who referred to linear combinations of binomial coefficients as "polyfracts") and continued by Clark and Schauz in [CS23]. Binomial coefficients were also used in lieu of polynomials in [BCC+17] for the purpose of extending the Ellenberg–Gijswijt bound on cap sets [EG17] to R^n; see also [Pet16] for an argument based on a more abstract concept of generalized polynomials, and [Spe16] 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 5.7, we prove that hyperplane functions in R^n are, in this sense, generalized n-variate polynomial functions 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*

$$\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}^*_{p^k,n}) \leqslant \binom{p^k - 1 + n}{n}. \tag{1.4}$$

However, unlike for $k = 1$, hyperplane functions in R^n with $k \geqslant 2$ 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 $k \geqslant 2$ and n is small relative to p^k.

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

$$\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{A}^*_{p^k,n}) \leqslant (2n)\binom{\lfloor p^k/2 \rfloor + (n-1)(p-1) + n}{n}, \tag{1.5}$$

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 $n \in \mathbb{N}$, $n \geqslant 2$. Then*

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

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

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 $|L \cap H| \equiv |L' \cap H| \bmod p$ for any hyperplane H; we prove in Proposition 9.3 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 9. 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.

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 Sections 3, 4, and 5.1, we define our generalized polynomials based on binomial coefficients and study their basic properties. (Many of them are special cases of the results in [AM21, CS22, CS23].) In Section 5.2, we prove that hyperplane functions in R^n have degree at most $p^k - 1$. In particular, Theorem 1.3 follows from Proposition 5.7.

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 $f(xy)$ can never be greater than $m + 2(p-1)$ (Proposition 6.2). This degree reduction is the main idea behind the proof of Theorem 1.4 in Section 7.

Finally, in Sections 8 and 9 we study the geometric properties of lines and hyperplanes in R^n, and develop the geometric test mentioned above.

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 $a \equiv b \bmod p^k$. When we work with functions with values in $\mathbb{Z}/p\mathbb{Z}$ (such as the ϕ_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 $R \to \mathbb{Z}/p\mathbb{Z}$, we will interpret a as the function $a \to (a \bmod p)$, 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 $x_1y_1 + \cdots + x_ny_n \equiv c \bmod p^k$ 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 $\mathbb{Z}/p\mathbb{Z}$. (We refer to $\langle f, g\rangle$ as the inner product, but this is a slight abuse of terminology, since for $k \geqslant 2$ it is not true that $\langle f, f\rangle = 0$ if and only if $f = 0$.)

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 $[m] = \{0, 1, \ldots, m-1\} \subset \mathbb{Z}$. 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 ℓ 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. Whenever we mention the p-adic expansion or p-adic digits of a number x, we refer to the unique expansion $x = \sum_{j=0}^{k-1} x_j p^j$ with $x_j \in \{0, 1, \ldots, p-1\}$ for all j. We use subscripts $1, \ldots, n$ to denote both the coordinates $x = (x_1, \ldots, x_n)$ 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. If a is either an integer or an element of R, we write $p^j \parallel a$ to mean $p^j \mid a$ but $p^{j+1} \nmid a$. Similarly, for $x = (x_1, \ldots, x_n) \in R^n$ or $\mathbb{Z}^n$, we write $p^j \parallel x$ if $p^j \mid x_i$ for all $i \in \{1, \ldots, n\}$ and $p^{j+1} \nmid x_i$ for at least one i.

2. Preliminary results

2.1. Relationships between incidence matrices

We first observe that

$$\operatorname{rank}(W^*_{p^k,n}) \leqslant \operatorname{rank}(W_{p^k,n}), \tag{2.1}$$

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 $k \geqslant 2$.

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

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

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

Let $y = (0, p^{k-1})$, 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

$$\mathbf{1}_{H_y} \notin \operatorname{span}(\mathcal{H}).$$

Assume towards contradiction that there are scalars α_i, β_j such that

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

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

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

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

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

we have

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

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

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

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

$$\operatorname{rank}(W_{p^k,n}) \leqslant 1 + \sum_{j=1}^{k} \operatorname{rank}(W^*_{p^j,n}), \tag{2.3}$$

and consequently,

$$\operatorname{rank}(W_{p^k,n}) \leqslant 1 + k \cdot \operatorname{rank}(W^*_{p^k,n}). \tag{2.4}$$

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

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

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

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

Note that the only vector in B_k is the zero vector, and so $W^{(k)}$ is a 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 $\operatorname{rank}(W^{(j)}) \leqslant \operatorname{rank}(W^*_{p^{k-j},n})$. 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 $\{x \in R^n : \langle x, b' \rangle = 0 \bmod p^k\}$. Recalling that $b' = p^j b$ for a direction b, we have

$$\langle x, b' \rangle = 0 \bmod p^k \quad \text{if and only if} \quad \langle x, b \rangle = 0 \bmod p^{k-j}. \tag{2.5}$$

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

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

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

Let $W^{(j)}_u$ be the submatrix of $W^{(j)}$ consisting of rows indexed by $x \in X_u$. By definition, for each u, the set $\{x \bmod p^{k-j} : x \in X_u\}$ can be identified with R^n_{k-j}. Similarly, the set $\{b : p^j b \in B_j\}$ can be identified with the set of directions of R^n_{k-j}. Combining these observations with the equivalence in (2.5), we see that $W^{(j)}_u$ 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.

Now inequality (2.4) follows from the bound $\operatorname{rank}(W^*_{p^j,n}) \leqslant \operatorname{rank}(W^*_{p^k,n})$ for $j < k$, which can be established by considering the submatrix of $W^*_{p^k,n}$ consisting of rows indexed by $x \in R^n$ that are zero mod p^{k-j}. □

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

$$\operatorname{rank}(\mathcal{A}^*_{p^k,n}) \leqslant \operatorname{rank}(W^*_{p^k,n+1}) \leqslant 2(k+1) \cdot \operatorname{rank}(\mathcal{A}^*_{p^k,n}). \tag{2.6}$$

Proof. We write directions $b \in R^{n+1}$ as $b = (\widetilde{b}, b_{n+1})$, with $\widetilde{b} \in R^n$. 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 $\operatorname{rank}(\mathcal{A}^*_{p^k,n}) \leqslant \operatorname{rank}(W^*_{p^k,n+1})$. Any affine hyperplane in R^n can be written as

$$\widetilde{H}_b = \left\{ \widetilde{x} \in R^n : \langle \widetilde{x}, \widetilde{b} \rangle = -b_{n+1} \right\}, \tag{2.7}$$

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

$$H_b = \left\{ x = (\widetilde{x}, x_{n+1}) \in R^{n+1} : \langle \widetilde{x}, \widetilde{b} \rangle + b_{n+1} x_{n+1} = 0 \right\}, \tag{2.8}$$

so that $\widetilde{H}_b \times \{1\} = H_b \cap \{x \in R^{n+1} : x_{n+1} = 1\}$. Consider the submatrix of $W^*_{p^k,n+1}$ obtained by restricting to rows indexed by $(\widetilde{b}, b_{n+1}) \in \mathcal{B} := \mathbb{P}R^{n-1} \times R$ 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 $j \in \{0, 1, \ldots, k\}$, let $X_j = \{x \in R^{n+1} : x_{n+1} = p^j y,\ y \neq 0 \bmod p\}$. Let $W^{(j)}$ be the submatrix of $W^*_{p^k,n+1}$ formed by restricting to the columns with $x \in X_j$. Then

$$\operatorname{rank}(W^*_{p^k,n+1}) \leqslant \sum_{j=0}^{k} \operatorname{rank}(W^{(j)}).$$

We will show that $\operatorname{rank}(W^{(j)}) \leqslant 2 \cdot \operatorname{rank}(A^*_{p^k,n})$ for each $j \in \{0, 1, \ldots, k\}$, implying the second bound in (2.6).

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,

$$\operatorname{rank}(W^{(j)}) \leqslant \operatorname{rank}(W_1^{(j)}) + \operatorname{rank}(W_2^{(j)}).$$

It therefore suffices to prove that

$$\operatorname{rank}(W_i^{(j)}) \leqslant \operatorname{rank}(\mathcal{A}^*_{p^k,n}) \text{ for } i = 1, 2. \tag{2.9}$$

We first prove (2.9) for $i = 1$. For each $b = (\widetilde{b}, b_{n+1}) \in \mathcal{B}$, let $H_b = \{x \in R^{n+1} : \langle x, b\rangle = 0\}$, and let

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

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

$$\operatorname{rank}(W_1^{(j)}) \leqslant \dim\left(\operatorname{span}\{\mathbf{1}_{H_b \cap X_j} : b \in \mathcal{B}_j\}\right), \tag{2.10}$$

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 $\widetilde{b}$ and the first $k - j$ digits in the p-adic expansion of b_{n+1}. Next, we prove that

$$\dim\left(\operatorname{span}\{\mathbf{1}_{H_b \cap X_j} : b \in \mathcal{B}_j\}\right) \leqslant \dim\left(\operatorname{span}\{\mathbf{1}_{\widetilde{H}_{b,j}} : b \in \mathcal{B}_j\}\right). \tag{2.11}$$

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 $H_b \cap X_k = \widetilde{H}_{b,k} \times \{0\}$ and the claim is clear.

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

$$\sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{\widetilde{H}_{b,j}} = 0. \tag{2.12}$$

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

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

First, we note that as s is invertible,

$$H_b \cap X_{j,s} = \{(s\widetilde{x}, sp^j) : \widetilde{x} \in \widetilde{H}_{b,j}\} \tag{2.13}$$

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 (2.13) and (2.12). Thus $\sum_{b \in \mathcal{B}_j} c_b \mathbf{1}_{H_b \cap X_j} = 0$, proving (2.11).

Combining (2.10) and (2.11), we get

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

as claimed.

To prove (2.9) for $i = 2$, we observe that if $b = (\widetilde{b}, b_{n+1}) \notin \mathcal{B}$, then $\widetilde{b}$ 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 $b = (b_1, \widetilde{b})$ for a direction $\widetilde{b} \in R^n$. The desired bound follows by the same argument as above with the first and last coordinates interchanged. □

2.2. Hyperplane matrices and Arsovski's matrix

Following [Ars24, Ars21], we define the matrix $M_{p^k,n}$, with both rows and columns indexed by elements of R^n, and with entries in $\mathbb{F}_p[z]/\langle z^{p^k} - 1\rangle$ given by

$$M_{p^k,n}(u, v) = z^{\langle u,v\rangle} \mod z^{p^k} - 1 \tag{2.14}$$

for $(u, v) \in R^n \times R^n$. Arsovski [Ars21] proved that the rank of $M_{p^k,n}$ over $\mathbb{Z}/p\mathbb{Z}$ is at least $p^{kn}(kn)^{-n}$. Dhar [Dha24] improved this to

$$\operatorname{rank}(M_{p^k,n}) \geqslant \binom{\lceil p^k/k \rceil + n}{n}. \tag{2.15}$$

Furthermore, in [Dha23a, Lemma 2.2.14, Observation 2.4.11] Dhar proved that

$$\operatorname{rank}(M_{p^k,n-1}) \leqslant \operatorname{rank}(W_{p^k,n}) \leqslant \operatorname{rank}(M_{p^k,n}). \tag{2.16}$$

The purpose of this section is to compare (2.16) to our upper bounds in Theorems 1.3 and 1.4. We will focus on $W_{p^k,n}$ since this is the matrix appearing in (2.16), but the bounds on the rank of $W^*_{p^k,n}$ and $\mathcal{A}^*_{p^k,n}$ are comparable, via (2.1), Proposition 2.2, and Proposition 2.3.

We start with upper bounds. By (2.15), any upper bound from (2.16) must be at least

$$U_1(k, n) := \binom{\lceil p^k/k \rceil + n}{n}.$$

Meanwhile, from (2.4), (2.6), and (1.4) we get

$$\operatorname{rank}(W_{p^k,n}) \leqslant 1 + 2k(k+1)\operatorname{rank}(\mathcal{A}_{p^k,n-1}) \leqslant 2k(k+2)\binom{p^k+n-2}{n-1} =: U_2(k,n).$$

We have

$$\begin{aligned}\frac{U_2(k,n)}{U_1(k,n)} &\leqslant 2k(k+2)n\frac{(p^k+n-2)(p^k+n-3)\dots p^k}{(p^kk^{-1}+n)(p^kk^{-1}+n-1)\dots(p^kk^{-1}+1)}\\ &\leqslant 2k(k+2)\frac{(p^k+n)^{n-1}}{p^{kn}k^{-n}}\\ &\leqslant 2k^{n+1}(k+2)\left(1+np^{-k}\right)^{n-1}p^{-k}.\end{aligned}$$

With n fixed, the bound $U_2(k,n)$ is better than $U_1(k,n)$ by a factor of the order $k^{n+2}p^{-k}$ for large p and k. Even if we used the easy bound (1.2) instead of $U_2(k,n)$, the outcome would be similar.

On the other hand, Theorem 1.3 shows that the lower bound in (2.16) provides the correct order of magnitude in p^k, up to constants depending on k and n. We have from (2.16) and (2.15)

$$\operatorname{rank}(W_{p^k,n}) \geqslant \binom{\lceil p^k/k\rceil+n-1}{n-1} =: L(k,n),$$

and

$$\begin{aligned}\frac{U_2(k,n)}{L(k,n)} &\leqslant 2k(k+2)\frac{(p^k+n-2)(p^k+n-3)\dots p^k}{(p^kk^{-1}+n-1)(p^kk^{-1}+n-2)\dots(p^kk^{-1}+1)}\\ &\leqslant 2k^n(k+2).\end{aligned}$$

When p^k is large relative to n, the bound in Theorem 1.4 improves this by an additional factor of up to 2^{n-1}. We provide the detailed calculation at the beginning of Section 7.

3. The binomial phi functions

In this section, we work in $R = \mathbb{Z}/p^k\mathbb{Z}$. Our starting point is Lucas's Theorem, which allows us to define binomial coefficients mod p as functions on R with values in $\mathbb{Z}/p\mathbb{Z}$.

Theorem 3.1 (Lucas's Theorem). *[Luc78] Let p be prime. Let m, n be nonnegative integers with p-adic expansions $m = \sum_{j=0}^{\ell} m_j$ and $n = \sum_{j=0}^{\ell} n_j p^j$, where $m_j, n_j \in [p]$. Then*

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

with the convention that $\binom{0}{0} = 1$ and $\binom{a}{b} = 0$ whenever $a, b \in [p]$ satisfy $a < b$.

Definition 3.2. For $m \in [p^k]$, we define the functions $\phi_m : R \to \mathbb{Z}/p\mathbb{Z}$ by

$$\phi_m(x) = \binom{x}{m} \bmod p, \tag{3.1}$$

with the same convention as in Theorem 3.1. We also define for all $x \in R$,

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

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

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

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

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

Proof. The first conclusion is trivial when $m < 0$ or $m \geqslant p^k$, since then $\phi_m(x) = 0$ for all x. Assume now that $m \in [p^k]$ and that $x \equiv y \bmod p^k$ for some $x, y \in \mathbb{Z}_{\geqslant 0}$. Then the p-adic expansions $x = \sum x_j p^j$ and $y = \sum y_j p^j$ satisfy $x_j = y_j$ for $0 \leqslant j \leqslant k-1$, 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. □

For $m = 0, 1, \ldots, p-1$, each ϕ_m coincides with the evaluation mod p of a polynomial in $R[z]$ of degree m. For $m \geqslant p$, (3.1) defines additional functions that can be thought of as "generalized polynomials" of degree m thanks to (3.3). An abstract framework for generalized polynomial functions on groups, defined as functions whose appropriate discrete derivatives are null, was developed by various authors, notably including [Lei02, Lac04, AM21, CS22]. A systematic study of binomial coefficients from this point of view was undertaken in [Sch14, CS23]. A large part of our analysis will follow theirs. However, for our purposes it will be important to consider *multiplicative* properties of binomial coefficients, which are significantly more complicated and were less studied in the literature (see the comments after equation (17) in [Sch14]).

We note that $\phi_0(x) = 1$ and $\phi_1(x) = x$ for all x, but ϕ_m with $2 \leqslant m < p$ are neither homogeneous nor monic. 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.

For $k = 1$, the polynomials $1, x, x^2, \ldots, x^{p-1}$ 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 ϕ_m for general k. This can be proved using the framework of discrete derivatives outlined in Section 4, but here we present a short and direct proof based on Lucas's Theorem.

Lemma 3.4. (Linear independence of ϕ_m) *We order the elements of R as $R = \{0, 1, 2, \ldots, p^k - 1\}$. Let Φ 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 Φ 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 Φ is an upper triangular matrix, nonsingular since all its diagonal entries are equal to 1. Since the m-th row of Φ is the list of values of $\phi_m(x)$ as $x \in R$, the linear independence of the rows of Φ implies the linear independence of ϕ_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. □

Vandermonde's identity (3.5) is the phi-function analogue of the binomial expansion of $(x + y)^m$.

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

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

Proof. Equation (3.5) is known in the literature. A short proof is as follows: the left side of (3.5) can be interpreted as the number of ways we can choose m balls from a basket of x white and y black balls, and the right side breaks this down into the numbers of ways we can choose i white balls and $m - i$ black balls for each i. □

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

$$\phi_{p^j m}(p^j x) = \phi_m(x). \tag{3.6}$$

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

Proof. This is an immediate consequence of (3.4). □

4. Discrete derivatives

In this section we study the properties of the phi functions with respect to discrete derivatives. Many of the properties we need may be found in [AM21] in a more general setting, and in [CS23, Sch14] specifically for binomial coefficients. Since the proofs are short, we include them for the reader's convenience.

Definition 4.1. For $m \in [p^k]$, define $\Omega_m := \text{span}\{\phi_\ell : 0 \leqslant \ell \leqslant m\}$. 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* ℓ if $f - g \in \Omega_\ell$; we write this as $f =_\ell g$.

For convenience, we set $\Omega_m := \{0\}$ for $m < 0$.

We define discrete derivatives as follows. For a function $f : R \to \mathbb{Z}/p\mathbb{Z}$, let

$$\Delta_c f(x) := f(x + c) - f(x) \text{ for } c \in R. \tag{4.1}$$

For short, we will also write $\Delta f = \Delta_1 f$. It follows from (3.3) that

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

By Lemma 3.4, any function $f : R \to \mathbb{Z}/p\mathbb{Z}$ has an expansion $f = \sum c_j\phi_j$. It follows from (4.2) that

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

Lemma 4.2. *Let $m \in [p^k]$ and $c \in R$. Then $\Delta_c\phi_m - c\phi_{m-1} \in \Omega_{m-2}$. Consequently, if $f \in \Omega_m$, then $\Delta_c f \in \Omega_{m-1}$ for all $c \in R$.*

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. □

A function $f : R \to \mathbb{Z}/p\mathbb{Z}$ has "functional degree" $m \geqslant 0$ in the sense of [AM21] if m is the smallest number such that $\Delta^{m+1} f$ is the zero function. Lemma 4.3 below states that this coincides[2] with the notion of the degree of f in Definition 4.1. The equivalence between (ii) and (iii) is a special case of [AM21, Lemma 2.2], and the equivalence between (i) and (ii) is contained in [Sch14, Theorem 3.1].

[2]Except for the zero function: in [AM21] it has degree zero, while we find it more convenient to assign it a negative degree.

Lemma 4.3. *For $m \in [p^k]$ and $f : R \to \mathbb{Z}/p\mathbb{Z}$, the following are equivalent:*

(i) $f \in \Omega_{m-1}$,

(ii) $\Delta^m f = 0$,

(iii) For any choice of $c_1, \ldots, c_m \in R$ we have $\Delta_{c_m} \ldots \Delta_{c_1} f = 0$.

Proof. The implication (i) $\Rightarrow$ (iii) follows by iterating Lemma 4.2 m times and using that $\Omega_{-1} = \{0\}$. Clearly (iii) implies (ii), by letting $c_1 = \cdots = c_m = 1$.

To prove that (ii) implies (i), we argue by contrapositive. Assume that $f : R \to \mathbb{Z}/p\mathbb{Z}$ has degree exceeding $m-1$. Then there is some $\ell \geqslant m$, 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

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

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

The remaining results in this section will be useful in studying the multiplicative properties of phi functions later on. Lemma 4.4 (i) is a special case of the periodicity results in [CS23, Section 2], [Sch14, Section 3]. Parts (ii) and (iii) are similar, but apply to functions that depend only on higher-order digits in the p-adic expansion of their variable.

Lemma 4.4. *Let $f : R \to \mathbb{Z}/p\mathbb{Z}$ 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 $\ell \in \{0, 1, \ldots, k-1\}$ Then:*

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

(ii) if $f(x) = g(x_\ell)$ for a function g of degree $m \in [p]$, then $f \in \operatorname{span}\{\phi_0, \phi_{p^\ell}, \phi_{2p^\ell}, \ldots, \phi_{mp^\ell}\}$;

(iii) $f(x)$ depends only on x_ℓ (that is, $f(x) = g(x_\ell)$ for some function $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$) if and only if $f \in \operatorname{span}\{\phi_0, \phi_{p^\ell}, \phi_{2p^\ell}, \ldots, \phi_{(p-1)p^\ell}\}$.

Proof. We start with (i). Suppose that f has degree at most $p^\ell - 1$. Then f is a linear combination of functions $\phi_m(x)$ with $m \leqslant p^\ell - 1$, so that $m_i = 0$ for all $i \geqslant \ell$. By Lucas's Theorem, f depends only on $x_0, x_1, \ldots, x_{\ell-1}$.

To prove the converse implication, we use dimension counting. There are p^ℓ functions ϕ_m with $m \leqslant p^\ell - 1$, all linearly independent, so that $\Omega_{p^\ell-1}$ has dimension p^ℓ. On the other hand, the space of all functions of $(x_0, x_1, \ldots, x_{\ell-1}) \in (\mathbb{Z}/p\mathbb{Z})^\ell$ also has dimension $|(\mathbb{Z}/p\mathbb{Z})^\ell| = p^\ell$. This proves (i).

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

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

by Lucas's Theorem, implying (ii). Part (iii) follows by observing that any function $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ has degree at most $p-1$ (Lemma 4.3 with $k = 1$) and then applying (ii) with $m = p - 1$. □

Lemma 4.5. *Let $\ell, m \in \mathbb{Z}_{\geqslant 0}$. Then $\phi_\ell \cdot \phi_m \in \Omega_{\ell+m}$, with*

$$\phi_\ell \cdot \phi_m =_{\ell+m-1} \binom{\ell+m}{\ell} \phi_{\ell+m}. \tag{4.3}$$

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 (4.3) could be zero. For example, if $\ell, m \leqslant p^j - 1$ for some $j < k$, then, by Lemma 4.4 (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 4.4 (i) again, $\phi_\ell\phi_m$ also has degree at most $p^j - 1$, even if $\ell + m \geqslant p^j$.

Proof of Lemma 4.5. The function $\phi_m : R \to \mathbb{Z}/p\mathbb{Z}$ is the reduction mod p of the polynomial $\binom{X}{m} \in \mathbb{Q}[X]$ with leading coefficient $(m!)^{-1}$. The polynomials

$$\binom{X}{m}\binom{X}{\ell} \quad \text{and} \quad \binom{\ell+m}{\ell}\binom{X}{\ell+m}$$

in $\mathbb{Q}[X]$ both have degree $\ell + m$ and both have the same leading coefficient $(m!\,\ell!)^{-1}$, so that their difference has degree at most $\ell + m - 1$. The function $\phi_\ell\phi_m - \binom{\ell+m}{\ell}\phi_{\ell+m}$ is the reduction mod p of that difference, therefore also has degree at most $\ell + m - 1$ as claimed. □

Lemma 4.6. *Let $\phi_m : R \to \mathbb{Z}/p\mathbb{Z}$ and $b \in R^\times$. Then*

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

Proof. The argument is similar to that in the proof of Lemma 4.5. The function $\phi_m(bx) - b^m\phi_m(x)$ is the reduction mod p of $\binom{bx}{m} - b^m\binom{x}{m}$, which is an integer-valued polynomial (with rational coefficients) of degree at most $m - 1$ in x. Therefore its reduction mod p also has degree at most $m - 1$. □

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. It has appeared in [Sch14, Theorem 2.6] (see also [Sch14, Theorem 2.7] and [CS23, Theorem 2.8 (b)] for a multivariate version).

Lemma 4.7. *Suppose that $f : R \to \mathbb{Z}/p\mathbb{Z}$ has the representation $f = \sum_{j=0}^{p^k-1} c_j\phi_j$. Then*

$$c_\ell = \Delta^\ell f(0) \text{ for all } \ell \in [p^k]. \tag{4.4}$$

Proof. By (4.2), we have

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

We now evaluate this at $x = 0$. Since $\phi_0(0) = 1$ and $\phi_j(0) = 0$ for all $j > 0$, we get (4.4). □

Corollary 4.8. *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 $f : R \to \mathbb{Z}/p\mathbb{Z}$ and $a \in R$, define $f^a(x) = f(ax)$. Then

$$(\Delta f^a)(x) = f(ax + a) - f(ax) = (\Delta_a f)(ax),$$

and, by iteration,

$$(\Delta^\ell f^a)(x) = (\Delta_a^\ell f)(ax) \text{ for all } \ell \in [p^k]. \tag{4.5}$$

The corollary follows by applying Lemma 4.7 to $f = \phi_m^a$ and then using (4.5). □

5. Phi functions on R^n

5.1. Phi functions as generalized polynomials

For $\alpha = (\alpha_1, \ldots, \alpha_n) \in [p^k]^n$, we define $\phi_\alpha : R^n \to \mathbb{Z}/p\mathbb{Z}$ by

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

Let also

$$\Omega_m^n := \operatorname{span}\{\phi_\alpha : |\alpha| \leqslant m\},$$

where $|\alpha| = \sum_i \alpha_i$. We say that a function $f : R^n \to \mathbb{Z}/p\mathbb{Z}$ 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

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

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

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

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

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

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

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

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

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

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

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 $\ell_1 + \cdots + \ell_{n+1} = L$. This in turn is equivalent to the following counting problem: given $L+n$ balls arranged in a row, colour L of them black and the remaining n white, so that the black balls divide the n white balls into $L+1$ subsets, with empty subsets permitted. The number of ways to do that is $\binom{L+n}{n}$. □

Proposition 5.4. *Let $g : R^n \to \mathbb{Z}/p\mathbb{Z}$ and $m \in \{0, 1, \dots, n(p^k - 1)\}$. Then the following are equivalent:*

(i) $g \in \Omega_d^m$,

(ii) *g has functional degree at most m, in the sense that for all $x \in R$ and for all $r^{(1)}, \dots, r^{(m+1)} \in R^n$ we have*

$$\Delta_{r^{(1)}} \dots \Delta_{r^{(m+1)}} f(x) = 0,$$

where $\Delta_r f(x) := f(x+r) - f(x)$ for $x, r \in R^n$.

We note here that, by [AM21, Lemma 8.1], the largest possible functional degree of a function $g : R^n \to \mathbb{Z}/p\mathbb{Z}$ is $n(p^k - 1)$; hence the upper bound on m in the proposition.

Proof of Proposition 5.4. It follows from [AM21, Lemma 6.2] that ϕ_α has functional degree at most $|\alpha|$. This proves that (i) implies (ii). For the converse, it suffices to prove that any function g of functional degree at most m may be represented as a linear combination of ϕ_α with $|\alpha| \leqslant m$. Such representation is provided by [CS23, Theorem 2.8 (b)] and [Sch14, Theorem 2.7].

Alternatively, one can also give a self-contained proof by induction in n, starting with Lemma 4.3 for $n = 1$ as the base case and then following essentially the same argument as in Lemmas 4.2 and 4.3 for the inductive step. The details are left to the reader. □

Corollary 5.5. *Let $g : R^n \to \mathbb{Z}/p\mathbb{Z}$ 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 $\{\phi_\alpha : |\alpha| \leqslant d\}$ is a basis for Ω_d^n, it follows that each ϕ_α with $|\alpha| \leqslant p-1$ 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 $d \leqslant p-1$ has functional degree at most d. By Proposition 5.4, we have $g \in \Omega_d^n$. Moreover, Ω_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 $|\alpha| \leqslant d$; see Lemma 5.3 above). Therefore the two spaces are equal. □

5.2. Phi functions and hyperplanes

Recall that

$$\mathcal{H}^n := \operatorname{span}\{\mathbf{1}_{H_b(a)} : \ a \in R^n, b \in \mathbb{P}R^{n-1}\} \tag{5.1}$$

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 5.6. *We have*

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

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

$$\begin{aligned}\operatorname{span}\{\mathbf{1}_{H_b(a)} : a \in R\} &= \operatorname{span}\{f(\langle x, b\rangle) : f \in (\mathbb{Z}/p\mathbb{Z})^R\} \\ &= \operatorname{span}\{\phi_\ell(\langle x, b\rangle) : \ell \in [p^k]\}.\end{aligned} \tag{5.2}$$

The second equality in (5.2) 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

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

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 $f : R \to \mathbb{Z}/p\mathbb{Z}$ 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 $i \in \{1, 2, \ldots, n\}$ 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 (5.2), and of the lemma. □

Proposition 5.7. *We have $\mathcal{H}^n \subset \Omega^n_{p^k-1}$ for all $k \geqslant 1$. In particular,*

$$\operatorname{rank}(\mathcal{A}^*_{p^k,n}) = \dim(\mathcal{H}^n) \leqslant \binom{p^k - 1 + n}{n}. \tag{5.3}$$

Proof. We prove that $\mathcal{H} \subset \Omega^n_{p^k-1}$ for all $k \geqslant 1$. By Lemma 5.6, it suffices to prove that $\phi_\ell(\langle b, x\rangle) \in \Omega^n_\ell$ for all $\ell \in [p^k]$ and $b \in \mathbb{P}R^{n-1}$. This follows from [AM21, Theorem 4.3]. An alternative self-contained proof is as follows: we use (3.5) to write

$$\phi_\ell(\langle b, x\rangle) = \sum_{|\alpha| \leqslant \ell} \phi_{\alpha_1}(b_1x_1) \cdots \phi_{\alpha_n}(b_nx_n). \tag{5.4}$$

Lemma 4.6 implies that $\phi_{\alpha_i}(b_i \cdot) \in \Omega_{\alpha_i}$ for each i. Hence each term on the right side of (5.4) has degree at most $|\alpha|$, which in turn implies that $\phi_\ell(\langle b, x\rangle) \in \Omega^n_\ell$ as claimed. The bound (5.3) follows from Corollary 5.2 with $m = p^k - 1$. □

For $k = 1$, we have the following stronger statement.

Proposition 5.8. *Let $k = 1$. Then $\mathcal{H}^n = \Omega^n_{p-1}$, and (5.3) holds with equality.*

The relation between polynomials and hyperplane indicator functions for $k = 1$ is well understood in the literature, see [GD68, MM68, Smi69]. The proof below is provided for completeness and for comparison with the case $k \geqslant 2$. We start with two preparatory lemmas. For $d \in [p]$, let $\mathcal{P}^n_{\leqslant d} := (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]_{\leqslant d}$ be the space of polynomials in n variables of degree at most d over $\mathbb{Z}/p\mathbb{Z}$, and let $\mathcal{P}^n_{=d}$ be the subspace of homogeneous, degree d polynomials in $\mathcal{P}^n_{\leqslant d}$.

Lemma 5.9. *Let $k = 1$. For any $n \in \mathbb{N}$ and any $d \in \{0, 1, \ldots, p-1\}$,*

$$\operatorname{span}\left\{\langle x, b\rangle^d : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}\right\} = \mathcal{P}^n_{=d}.$$

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

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

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

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

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

Therefore it suffices to show that

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

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

$$\left\{\langle \widetilde{x}, c\rangle^j x_n^{d-j} : j = 0, 1, \ldots, d-1\right\} \subset \operatorname{span}\left\{\langle x, (c, i)\rangle^d - (ix_n)^d : i = 1, \ldots, d\right\}, \tag{5.5}$$

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

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

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

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

where we evaluated the determinant of the Vandermonde matrix. Since $\binom{d}{j} \neq 0$ for $d \leqslant p-1$, our coefficient matrix is nonsingular, so that we can solve for $\langle \widetilde{x}, c\rangle^{d-j} x_n^j$ as claimed in (5.5). $\square$

Lemma 5.10. *Let $k = 1$. For any $d \in \{0, 1, \ldots, p-1\}$, we have*

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

Proof. By Lemma 5.9, it suffices to show that

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

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,

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

Consider the system of equations

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

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

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

This is non-zero as in the proof of Lemma 5.9, hence we can solve for $\langle x, b\rangle^{d-j}$. □

Proof of Proposition 5.8. Let $k = 1$. Observe that the indicator function of a hyperplane $H_b(a)$ may be written as $\mathbf{1}_{H_b(a)}(x) = 1 - \langle x - a, b\rangle^{p-1} \bmod p$. By Lemma 5.10 with $d = p - 1$, we have $\mathcal{H}^n = \mathcal{P}^n_{\leqslant p-1}$. It follows by Corollary 5.5 that $\mathcal{H}^n = \Omega^n_{p-1}$, as claimed. □

Proof of Theorem 1.2. Let $\mathcal{H}^n_0 = \operatorname{span}\{\mathbf{1}_{H_b} : b \in \mathbb{P}(\mathbb{Z}/p\mathbb{Z})^{n-1}\}$ be the span of homogeneous hyperplane functions. The same argument as above, but using Lemma 5.9 instead of 5.10, shows that $\mathcal{H}^n_0$ 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 homogeneous hyperplane functions. Such representation is provided by

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

Note that this equality needs only to hold modulo p: the subspace $x_1 = x_2 = 0$ appears in all $p + 1$ hyperplanes above, for a contribution 1 mod p. □

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 $i,j \geqslant 1$, 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 4.4 (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

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

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 $i \leqslant j$.

- If $i < j$, then $p^{i+1} \leqslant p^j$, so that $p^{i+1} + p^{j+1} - p^i - p^j \leqslant p^{j+1} - p^i < p^{i+j}$.
- If $i = j \geqslant 2$, then $2p^{i+1} - 2p^i < 2p^{i+1} \leqslant p^{i+2} \leqslant p^{i+j}$.
- 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
$$\phi_1(x_1 y_1) = x_1 y_1 = \phi_p(x)\phi_p(y)$$
has degree $2p \leqslant p^2$, 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 4.8 that

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

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 4.6, $\phi_m(iy)$ 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*

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

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

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

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

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

By Lemma 6.1, P_3 has degree at most

$$\sum_{i,j\geqslant 1} m_{ij} p^{i+j}. \tag{6.3}$$

Next, we consider P_1. By (6.1) and Lemma 4.4, 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 $\beta_2 \leqslant m_{0j} p^j$. Taking the product, and applying Lemma 4.4 to the factors involving x_0 and Lemma 4.5 to the factors involving y, we see that P_1 has degree at most

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

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. □

7. An upper bound on the rank of hyperplane functions

In this section we prove our upper 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*

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

Before starting the proof of the theorem, we compare (7.1) to the upper bound $\binom{p^k-1+n}{n}$ given by (5.3). Suppose that n is small relative to p^{k-1}, with $n < \epsilon p^{k-1}$ for some $\epsilon > 0$. Then

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

Meanwhile, we have

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

Hence, for $n < \epsilon p^{k-1}$, the estimate in (7.1) improves on that in Proposition 5.3 by a factor of at least $n2^{-(n-1)}(1+4\epsilon)^n$.

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 (5.1). By Lemma 5.6, we further have

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

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

$$\operatorname{rank}(\mathcal{A}^*_{p^k,n}) \leqslant n \cdot \operatorname{rank}(\mathbb{H}^{(n)}), \tag{7.3}$$

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

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

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

$$\begin{aligned} \phi_m(\langle \widetilde{a}, \widetilde{x}\rangle + x_n) &= \sum_{\ell_1+\dots+\ell_{n-1}+\beta_n = m} \phi_{\ell_1}(a_1x_1)\cdots\phi_{\ell_{n-1}}(a_{n-1}x_{n-1})\phi_{\beta_n}(x_n) \\ &= \sum_{\ell_1+\dots+\ell_{n-1}+\beta_n = m} \sum_{\widetilde{\alpha},\widetilde{\beta}} \gamma(\widetilde{\ell}, \widetilde{\alpha}, \widetilde{\beta})\phi_{\widetilde{\alpha}}(\widetilde{a})\phi_\beta(x), \end{aligned} \tag{7.4}$$

where we write

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

and

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

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

Let Φ 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 Ψ be the block-diagonal matrix with rows indexed by $(m, \widetilde{a}) \in [p^k]^n$, columns indexed by $(\mu, \widetilde{\alpha}) \in R^n$, and entries

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

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 $(m, \widetilde{\alpha}) \in R^n$, columns indexed by $\beta \in [p^k]^n$, and entries

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

Since both Φ and Ψ 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. □

Proposition 7.2. *We have*

$$\operatorname{rank}\left(\mathbb{B}^{(n)}\right) \leqslant 2\binom{\lfloor p^k/2\rfloor + (n-1)(p-1) + n}{n}.$$

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

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

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

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

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 $\gamma(\widetilde{\ell}, \widetilde{\alpha}, \widetilde{\beta}) = 0$. Since this is true for all contributing terms, the claim follows.

Write $|\widetilde{\alpha}| = \sum_{j=1}^{n-1} \alpha_j$ 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, $\mathbb{B}^{(n)}_{\leqslant\lambda}$ and $\mathbb{B}^{(n)}_{>\lambda}$, with rows and columns indexed as for $\mathbb{B}^{(n)}$.

Let $\mathbb{B}^{(n)}_{\leqslant\lambda}$ be defined so that for any row indexed by $(m,\widetilde{\alpha})$ with $m-|\widetilde{\alpha}|\leqslant\lambda$, the $(m,\widetilde{\alpha})$-row of $\mathbb{B}^{(n)}_{\leqslant\lambda}$ matches the $(m,\widetilde{\alpha})$-row of $\mathbb{B}^{(n)}$. All other rows are zero. Then define $\mathbb{B}^{(n)}_{>\lambda}$ so that

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

First consider $\mathbb{B}^{(n)}_{\leqslant\lambda}$. All its non-zero entries lie in rows indexed by $(m,\widetilde{\alpha})$ with $m-|\widetilde{\alpha}|\leqslant\lambda$. By (7.6), any column indexed by β 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

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

by Lemma 5.3.

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

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

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

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

□

8. The basics of finite p-adic geometry

We saw in Theorem 7.1 that functional degree provides only a partial characterization of hyperplane functions. In order to develop additional geometric conditions, we need some basic facts about lines, planes, and their intersections in finite p-adic geometry. The material here is likely familiar to experts (p-adic scales are used in a similar way in the literature on variants of the Kakeya problem, see e.g. [HW18, Section 4.3]), but we did not find a self-contained exposition of all the facts we need, so we provide them with proofs in this section. The language of angles and distances, defined below, provides the geometric intuition for setting up and understanding the constructions in Section 9.

8.1. Lines, planes, distances, angles

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 $1 \leqslant \ell \leqslant k$, so that $R_k = R$ and $R_1 = \mathbb{Z}/p\mathbb{Z}$.

We define distances and angles in R as follows. For $x = (x_1, \dots, x_n) \in R^n$, we recall that $p^j \parallel x$ means that $p^j \mid x_i$ for all $i \in \{1, \dots, n\}$ and $p^{j+1} \nmid x_i$ for at least one i. We will say that the *p-adic distance* between two distinct points $x, y \in R^n$ is p^{-j} if $p^j \parallel x - y$, and write it as $\|x - y\| = p^{-j}$.

The angle between two directions b, b' is the p-adic distance between b and b' in $\mathbb{P}R^{n-1}$. Equivalently: given two distinct directions $b, b' \in \mathbb{P}R^{n-1}$, we say that the *$p$-adic angle* between b and b' is at most p^{-j}, and write $\angle(b, b') \leqslant p^{-j}$, if there exist representatives rb and $r'b'$ with $r, r' \in R^\times$ such that $p^j \mid (rb - r'b')$. We say that $\angle(b, b') = p^{-j}$ if $\angle(b, b') \leqslant p^{-j}$ but $\angle(b, b') \not\leqslant p^{-j-1}$. The following simple observation will be used in the sequel.

Lemma 8.1. *(cf. [Car18, Corollary 1.11]) Let $b, b' \in \mathbb{P}R^{n-1}$. Then $\angle(b, b') = 1$ if and only if*

$$\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}} \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b'_1 & b'_2 & \dots & b'_n \end{pmatrix} = 2.$$

Proof. The equation above is equivalent to the statement that no linear combination $cb + c'b'$ with $c, c' \in R^\times$ is congruent to the zero vector mod p, which is a restatement of the definition of angle 1. □

It will be convenient to say that $\|x - x\| = p^{-k}$ and $\angle(b, b) = p^{-k}$; with that convention, results such as Lemma 8.2 below continue to hold when $j = k$. In the sequel, we will usually say "angle" and "distance" for short instead of "p-adic angle" and "p-adic distance".

For $0 \leqslant \ell \leqslant k$, define a *$p^{-\ell}$-cube* to be a set of the form

$$Q = Q_\ell(x) = \{y \in R^n : p^\ell \mid (y - x)\},$$

for a fixed $x \in R^n$. This is the set of those elements of R^n whose distance from x is at most $p^{-\ell}$. In dimension $n = 2$, we refer to Q as a square. Note that a 1-cube $Q_0(x)$ is the entire R^n, and a p^{-k}-cube $Q_k(x)$ is the singleton $\{x\}$.

We can visualize $(\mathbb{Z}/p^k\mathbb{Z})^2$ as a p-adic grid; in the table below, we give an example with $p = 2$, $k = 2$, where points can be organized according to four p^{-1}-squares, $Q_1(0, 0)$, $Q_1(1, 0)$, $Q_1(0, 1)$, and $Q_1(1, 1)$:

	0	2	1	3
0				
2				
1				
3				

A *line* in a nondegenerate direction $b \in \mathbb{P}R^{n-1}$ is a set of the form

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

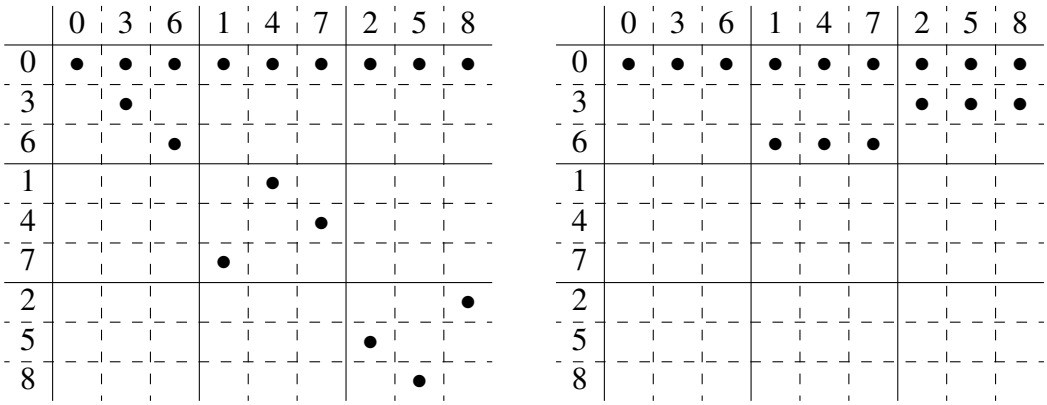

Figure 8.1: Examples with (a) two lines with p-adic angle equal to 1, and (b) two lines with p-adic angle equal to p^{-1}. In (a), the two lines share the point $(0,0)$. In (b), the lines share the three points $(0,0), (3,0), (6,0)$.

In this article, we only consider lines as defined above, with $b \in \mathbb{P}R^{n-1}$. Thus a line $L_b(a)$ is always assumed to be nondegenerate and always has $|R| = p^k$ distinct elements; furthermore, if $x = a + tb$, then $p^\ell | (x-a) = tb$ if and only if $p^\ell | t$, so that

$$L_b(a) \cap Q_\ell(a) = \{a + tb : \ p^\ell | t\}, \tag{8.1}$$

and in particular

$$|L_b(a) \cap Q_\ell(a)| = p^{k-\ell} \text{ for } 0 \leqslant \ell \leqslant k.$$

If L and L' are lines with directions b and b' respectively, we define the angle between them to be $\angle(L, L') = \angle(b, b')$.

In Figure 8.1, we give an examples of pairs of lines in $\mathbb{Z}/3^2\mathbb{Z}$ with p-adic angles equal to 1, and then angle equal to 3^{-1}. The lines in the first example have directions $(1,0)$ and $(4,1)$, while in the second, the lines have direction $(1,0)$ and $(1,6)$.

A *2-plane* in R^n is a set of the form

$$\Pi_{v,v'}(a) = \{a + tv + t'v' : \ t, t' \in R\}$$

for some $a \in R^n$ and $v, v' \in \mathbb{P}R^{n-1}$ such that $\angle(v, v') = 1$. In other words, it is a coset of a subgroup of R^n with two generators and maximal size $|R|^2 = p^{2k}$.

The next two lemmas justify our geometric terms for angles and distances. Analogous results hold in $\mathbb{R}^n$ if one replaces lines by tubes[3] of small but positive radius. For example, if the central axes of two such tubes intersect at an angle θ, then the intersection of the tubes has volume inversely proportional to θ and is contained in a $O(\theta^{-1})$-neighbourhood of the intersection point of the axes; Lemma 8.2 is the analogous result in our setting. Lemma 8.3 is a similar statement about lines intersecting hyperplanes at an angle.

[3]This is often done in projection theory and Kakeya-type problems.

Lemma 8.2. *(cf. [HW18, Lemma 4.5]) Let $L, L' \subset R^n$ be lines. Assume that L and L' have a point in common, so that $L = L_b(a)$ and $L' = L_{b'}(a)$ for some $a \in R^k$ and some choice of directions b, b'. If $\angle(L, L') = p^{-j}$ for some $0 \leqslant j \leqslant k$, then*

$$L \cap L' = L \cap Q_{k-j}(a) = L' \cap Q_{k-j}(a).$$

In particular, $|L \cap L'| = p^j$.

Proof. Let $L = L_b(a)$ and $L' = L_{b'}(a)$, with b, b' chosen so that $p^{-j} \parallel (b - b')$. We first prove that

$$L \cap L' \subset Q_{k-j}(a). \tag{8.2}$$

Suppose that $x \in L \cap L'$ satisfies $x \neq a$ and $p^\ell \parallel (x - a)$ for some $0 \leqslant \ell < k$. We have $x = a + tb = a + sb'$ for some $s, t \in R$. Since $x - a = tb = sb'$ and b, b' are both nondegenerate, we must have $p^\ell \parallel t$ and $p^\ell \parallel s$. Therefore there exists $c \in R^\times$ such that $t = cs$.

Let $b'' = c^{-1}b'$, then b'' represents the same direction as b' and

$$x = a + tb = a + sb' = a + s(cb'') = a + tb''.$$

Hence $tb = tb''$, and by the definition of angle, p^j is the highest power of p that may divide $b - b''$. It follows that $p^{k-j} | t$, so that $p^{k-j} \mid tb = x - a$, as claimed.

It is left to prove that $L \cap Q_{k-j}(a) \subset L \cap L'$, and similarly for L'. Let $x = a + tb \in L \cap Q_{k-j}(a)$. By (8.1), we have $p^{k-j} | t$. Then $(a + tb) - (a + tb') = t(b - b')$ is divisible by $p^{k-j}p^j = p^k$, hence is the zero element in R^n. It follows that $x = a + tb' \in L'$. The same argument applies with L and L' interchanged. □

Lemma 8.3. *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 $a \in L \cap H$, and that $\langle b, v\rangle = cp^j$ for some invertible $c \in R^\times$ and $0 \leqslant j \leqslant k$. Then $L \cap H = L \cap Q_{k-j}(a)$, and in particular $|L \cap H| = p^j$.*

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

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

This holds if and only if $p^{k-j} \mid t$, and the conclusion follows from (8.1). □

Lemma 8.4. *The following are true:*

(i) Let L, L' be lines in R^2. If $\angle(L, L') = 1$, then $|L \cap L'| = 1$.

(ii) Let Π be a 2-plane and H a hyperplane in R_1^n. Assume that $\Pi \cap H \neq \varnothing$. Then either $\Pi \subset H$, or else $\Pi \cap H$ is a line.

Proof. For (i), let $L = L_b(a)$ and $L' = L_{b'}(a')$. We need to verify that the equation $a + tb = a' + sb'$, or equivalently

$$\begin{pmatrix} b_1 & -b_1' \\ b_2 & -b_2' \end{pmatrix} \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} a_1' - a_1 \\ a_2' - a_2 \end{pmatrix}$$

has a unique solution $(t, s) \in R^2$. This follows from Lemma 8.1.

For (ii), let $H = H_a(b)$ and $\Pi = \Pi_{v,v'}(a)$ for some $a \in R_1^n$. If $\langle v, b\rangle = \langle v', b\rangle = 0$, then $\Pi \subset H$. Otherwise, it is easy to check that $\Pi \cap H = L_u(a)$, where

$$u = \langle v, b\rangle v' - \langle v', b\rangle v.$$

□

8.2. Projections and scaling

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

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

Clearly, the mappings π_ℓ are linear, and $\pi_\ell(x) = \pi_\ell(y)$ if and only if $\|x-y\| \leqslant p^{-\ell}$. The projection π_ℓ induces a mapping $\mathbb{P}R^{n-1} \to \mathbb{P}R_\ell^{n-1}$ that we will also denote by π_ℓ, with $\pi_\ell(b) = \pi_\ell(b')$ if and only if $\angle(b,b') \leqslant p^{-\ell}$. In terms of p-adic digit expansions: given ℓ as above, any element $x \in R^n$ may be represented uniquely as

$$x = x_* + p^\ell x^* \bmod p^k, \text{ where } x_* \in [p^\ell]^n,\ x^* \in [p^{k-\ell}]^n. \tag{8.3}$$

With this notation, we have $\pi_\ell(x) = (x_* \bmod p^\ell) \in R_\ell^n$.

We will continue to use our notation for lines, 2-planes, and hyperplanes on lower scales: for example, if $\tilde{a} \in R_\ell^n$ and $\tilde{b} \in \mathbb{P}R_\ell^{n-1}$, we will write $L_{\tilde{b}}(\tilde{a})$ to denote the line $\{\tilde{a} + t\tilde{b} :\ t \in R_\ell\}$ in R_ℓ^n.

Lemma 8.5 (Properties of π_ℓ)**.** *Let $0 \leqslant \ell \leqslant k-1$, $a \in R^n$, and $b, b' \in \mathbb{P}R^{n-1}$ with $\angle(b,b') = 1$. Then:*

(i) $\pi_\ell(L_b(a)) = L_{\pi_\ell(b)}(\pi_\ell(a))$,

(ii) $\pi_\ell(H_b(a)) = H_{\pi_\ell(b)}(\pi_\ell(a))$,

(iii) $\pi_\ell(\Pi_{b,b'}(a)) = \Pi_{\pi_\ell(b),\pi_\ell(b')}(\pi_\ell(a))$.

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), we use the representation (8.3) for x, a, b. Then

$$\langle x-a, b\rangle = \langle x_* - a_*, b_*\rangle + p^\ell(\langle x_* - a_*, b^*\rangle\rangle + \langle x^* - a^*, b\rangle).$$

If $x \in H_b(a)$, it follows that $\langle x_* - a_*, b_*\rangle \equiv 0 \bmod p^\ell$, so that $\pi_\ell(x) \in H_{\pi_\ell(b)}(\pi_\ell(a))$. Conversely, suppose that $x_* \in [p^\ell]$ satisfies $\langle x_* - a_*, b_*\rangle = 0 \bmod p^\ell$. Then for any x^* satisfying

$$\langle x_* - a_*, b^*\rangle + \langle x^* - a^*, b\rangle = 0 \bmod p^{k-\ell},$$

we have $x := x_* + x^* p^\ell \in H$ (notice that such an x^* must exist as b is non-zero mod p). This completes the proof of (ii). The proof of (iii) is similar. □

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 p^{-1}-cube Q. Then $L \cap L' \subset Q$.*

Proof. Suppose L and L' intersect at a point in some p^{-1}-cube Q'. Then the lines $\pi_1(L)$ and $\pi_1(L')$ in R_1^n pass through both of the points $q' = \pi_1(Q')$ and $q = \pi_1(Q)$. 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 $Q = Q'$. □

Next, we establish a canonical identification of a $p^{-\ell}$-cube in R^n with $R^n_{k-\ell}$. Let Q be a $p^{-\ell}$-cube. We recall the representation (8.3) of elements of R^n. Note that if $x, y \in Q$, then (with the obvious notation) we have $y_* = x_*$. This allows us to define the map $\iota_Q : Q \to R^n_{k-\ell}$ via

$$\iota_Q(x) = (x^* \bmod p^{k-\ell}).$$

Clearly, ι_Q is not a linear mapping, since Q is not closed under addition or scalar multiplication to begin with. However, it is a rescaling, and it maps intersections of affine subspaces with Q to affine subspaces in $R^n_{k-\ell}$. The precise statement is given in Lemma 8.7 below.

Lemma 8.7. (Properties of ι_Q) *Let Q be a $p^{-\ell}$-cube in R^n for some $0 \leqslant \ell \leqslant k-1$. Let $a \in Q$ and $b, b' \in \mathbb{P}R^{n-1}$ satisfy $\angle(b, b') = 1$. Then:*

(i) If $L = L_b(a) \subset R^n$, then $\iota_Q(Q \cap L) = L_{\pi_{k-\ell}(b)}(\iota_Q(a))$ is a line in $R^n_{k-\ell}$.

(ii) If $H = H_b(a) \subset R^n$, then $\iota_Q(Q \cap H) = H_{\pi_{k-\ell}(b)}(\iota_Q(a))$ is a hyperplane in $R^n_{k-\ell}$.

(iii) If $\Pi = \Pi_{b,b'}(a) \subset R^n$, then $\iota_Q(Q \cap \Pi) = \Pi_{\pi_{k-\ell}(b),\pi_{k-\ell}(b')}(a)$ is a 2-plane in $R^n_{k-\ell}$.

Proof. We recall the representation (8.3) of elements of R^n. For (i), we have by (8.1)

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

so that

$$\iota_Q(Q \cap L) = \{a^* + \lambda \pi_{k-\ell}(b) : \lambda \in R_{k-\ell}\} = L_{\pi_{k-\ell}(b)}(\iota_Q(a)) \subset R^n_{k-\ell}$$

as claimed. Next, similar to (8.1) we have

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

and so

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

The proof of (iii) is similar. □

9. Geometric test for hyperplane functions

9.1. Fans

We saw in Proposition 5.7 that hyperplane functions have degree at most $p^k - 1$. In other words, if $f \in \mathcal{H}^n$, then for any choice of $a, r_1, \ldots, r_{p^k} \in R^d$ we have

$$\left\langle f,\ \sum_{\vec{\epsilon}} (-1)^{|\vec{\epsilon}|} \mathbf{1}_{x_{\vec{\epsilon}}} \right\rangle = 0, \tag{9.1}$$

where the summation is over all $\vec{\epsilon} = (\epsilon_1, \ldots, \epsilon_{p^k}) \in \{0,1\}^{p^k}$, and

$$|\vec{\epsilon}| = \sum_{j=1}^{p^k} \epsilon_j, \quad x_{\vec{\epsilon}} = a + \sum_{j=1}^{p^k} \epsilon_j r_j. \tag{9.2}$$

However, Theorem 7.1 tells us that $\mathcal{H}^n$ is in general significantly smaller than the linear space of functions of degree less than p^k. This raises the question of what other functions $\psi : R^n \to \mathbb{Z}/p\mathbb{Z}$ might be orthogonal to $\mathcal{H}^n$, in the sense that $\langle f, \psi \rangle = 0$ for all $f \in \mathcal{H}^n$. We now define one class of such functions. We continue to use the notation from Section 8.

Definition 9.1 (Fans)**.** Let $0 \leqslant \ell \leqslant k-2$. For $a \in R^n$, let $Q = Q_{\ell+1}(a)$, $Q' = Q_\ell(a)$, and let Π be a 2-plane passing through a. Let $L_0, \ldots, L_p$ be lines passing through a, contained in Π, and satisfying $\angle(L_i, L_j) = 1$ for each $i \neq j$. Then the set

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

is a *fan* on scale ℓ.

By Lemma 8.4, for all $i \neq j$ we have $L_i \cap L_j = \{a\} \subset Q$, so that

$$(L_i \cap X) \cap (L_j \cap X) = \varnothing \text{ for } i \neq j. \tag{9.3}$$

We also note that, by (8.1),

$$|X| = \sum_{j=0}^{p} |(L_j \cap Q') \setminus Q| = (p+1)(p^{k-\ell} - p^{k-\ell-1}) \tag{9.4}$$

Theorem 9.2. *Assume that $k \geqslant 2$. Let $f \in \mathcal{H}^n$ be a hyperplane function, and let $X \subset R^n$ be a fan. Then*

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

To prove the theorem, it suffices to prove that $|H \cap X| = 0 \bmod p$ for any hyperplane H and any fan X. We prove this in Section 9.2 for $n = 2$ and $\ell = 0$, and in Section 9.3 in the general case.

We prove in Section 9.4 that there are functions ϕ_α with $|\alpha| \leqslant p^k - 1$ that are not orthogonal to appropriately selected fans. Thus, fans can (at least sometimes) distinguish between genuine hyperplane functions and functions that have degree bounded by $p^k - 1$ but are not in $\mathcal{H}^n$. This also proves that fans do not belong to the linear span of the test functions in (9.1)–(9.2).

It is an interesting question to determine whether there are any functions, other than linear combinations of fans and test functions from (9.1)–(9.2), that are orthogonal to all hyperplane functions. It could also be interesting to determine the dimension of the linear span of fans. However, this would not be likely to lead to an improved upper bound on the dimension of $\mathcal{H}^n$. First, the dimension of the linear span of fans appears at least as difficult to determine as that of $\mathcal{H}^n$. Second, even if we could determine the former, the inner product in R^n does not have the property that $\langle f, f \rangle = 0$ if and only if $f = 0$. (For example, we have $\langle f, f \rangle = 0$ if f is the indicator function of any set of cardinality divisible by p.) Hence the dimension of a space of functions from R^n to $\mathbb{Z}/p\mathbb{Z}$ is not determined by the dimension of its orthogonal complement.

We note that functions of degree at most $p^k - 1$ share some of the geometric properties of hyperplane functions. For example, if L, L' are two lines in R^n with $\angle(L, L') < 1$,

then $|L \cap H| \equiv |L' \cap H| \bmod p$ for any hyperplane H. In Section 9.5, we prove a similar statement for functions of degree up to $p^k - 1$. This also implies that Theorem 9.2 would remain true if we allowed a more general definition of fans where, instead of all lines passing through the same point a and lying in a fixed 2-plane Π, we only required all L_i to pass through Q and lie in the $p^{-\ell-1}$-neighbourhood of Π.

We are not aware of any instance of fans defined or used previously in the literature in any similar context. We do not know whether they have a functorial interpretation, similar to the association of the test functions in (9.1)–(9.2) with discrete derivatives. That could be another interesting question to consider.

9.2. Proof for $n = 2$ and $\ell = 0$

Let $a \in R^2$. Let $\mathcal{L} = \{L_0, L_1, \dots, L_p\}$ be a collection of $p+1$ lines in R^2 such that $a \in L_j$ for all $j \in \{0, 1, \dots, p\}$, and that $\angle(L_i, L_j) = 1$ for any $i \neq j$. Note that if B is the set of directions of the lines in $\mathcal{L}$, then

$$\{b \bmod p : \ b \in B\} = \{(0,1), (1,0), (1,1), \dots, (1, p-1)\},$$

so that B is a maximal 1-separated set of directions in $\mathbb{P}R$.

Let $Q = Q_1(a)$, and $X = \bigcup_{i=0}^{p} L_i \setminus Q$. Since hyperplanes in R^2 are lines (recall our convention that both hyperplanes and lines are nondegenerate unless specified otherwise), we need to prove that for any line L in R^2 we have

$$|L \cap X| = 0 \bmod p.$$

Let L be a line in R^2. By (9.3), we have

$$|L \cap X| = \sum_{i=0}^{p} |L \cap L_i \cap X|. \tag{9.5}$$

Note also that there is a unique line L_i in $\mathcal{L}$ such that $\angle(L, L_i) < 1$; without loss of generality, assume $i = 0$.

First suppose that $L \cap Q = \varnothing$. By Lemma 8.4, for each $i \in \{1, \dots, p\}$, L intersects L_i at a unique point $p_i \notin Q$, so that $|L \cap L_i \cap X| = 1$ for $i = 1, \dots, p$. Next, we have $|L \cap L_0 \cap X| = \sum |L \cap L_0 \cap \widetilde{Q}|$, where the summation is over all p^{-1}-squares $\widetilde{Q} \neq Q$. By Lemma 8.2, each term $|L \cap L_0 \cap \widetilde{Q}|$ is 0 mod p, hence $|L \cap L_0 \cap X| = 0 \bmod p$. Combining this all with (9.5), we obtain $|L \cap X| = 0 \bmod p$, as desired.

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

9.3. Proof in the general case

Define X and all its associated objects as in Definition 9.1, and let H be a hyperplane. We need to prove that

$$|H \cap X| \equiv 0 \mod p. \tag{9.6}$$

We first consider the case when $\ell = 0$, so that $Q' = R^n$. If $H \cap X = \varnothing$, there is nothing to prove. Otherwise, we have $H \cap \Pi \neq \varnothing$. By Lemma 8.4, either $\Pi \subset H$, or else $\Pi \cap H$ is a line. In the first case, we have $H \cap X = X$, and

$$|H \cap X| = |X| = (p+1)(p^k - p^{k-1}),$$

which is divisible by p since $k \geqslant 2$.

Assume now that $\Pi \cap H$ is a line. Suppose that $\Pi = \Pi_{v,v'}(a)$ for some $v, v' \in \mathbb{P}R^{n-1}$ with $\angle(v, v') = 1$. By Lemma 8.1, there is a nonsingular linear transformation $F : R^n \to R^n$ such that $F(v) = e_1 := (1, 0, \ldots, 0)$ and $F(v') = e_2 := (0, 1, 0, \ldots, 0)$. Then $F(X)$ is a fan in $F(\Pi)$, and $F(\Pi \cap H)$ is a line in $F(\Pi)$. Identifying $F(\Pi)$ with R^2 in the obvious way, and applying the result for $n = 2$, we get that (9.6) holds in this case.

Finally, if $\ell > 0$, let $\iota_{Q'} : Q' \to R^{k-\ell}$ be the identification mapping defined in Section 8.2. By Lemma 8.7, $\iota_{Q'}(X)$ is a fan on scale 0 in $R^{k-\ell}$, and $\iota_{Q'}(H)$ is a hyperplane in $R^{k-\ell}$. By the $\ell = 0$ case of the theorem, we have $|\iota_{Q'}(H) \cap \iota_{Q'}(X)| = 0 \bmod p$. Since $\iota_{Q'}$ is a bijection, (9.6) follows.

9.4. An example

We let $n = 2$, $k \geqslant 2$, and use (x, y) to denote elements of R^2 so that $x, y \in R$. Let

$$f(x, y) = \phi_{p^k - p^{k-1}}(x)\phi_{p^{k-1} - p^{k-2}}(y) = \phi_{p-1}(x_{k-1})\phi_{p-1}(y_{k-2}), \tag{9.7}$$

where $x = \sum_i x_i p^i$ and $y = \sum_i y_i p^i$ are the usual p-adic expansions of x and y. Thus f is the indicator function of the set

$$Y = \{(x, y) \in R^2 : \ x_{k-1} = p - 1, \ y_{k-2} = p - 1\}.$$

As a specific example, let $p = k = 2$. We list 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.

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 ϕ_{21} as a linear combination of several hyperplane functions. Theorem 9.2 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

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

More generally, the function f defined in (9.7) has degree $p^k - 1$. However, Theorem 9.2 shows that is not a hyperplane function. Let $\ell = k-2$ and $a = (p^k - p^{k-1}, p^{k-1} - p^{k-2})$. Let $L_0, L_1, \ldots, L_{p-1}, L_p$ be the lines through a in the direction of $(1,0), (1,1), \ldots, (1,p-1)$, and $(0,1)$, respectively. Let X be the fan

$$X = \bigcup_{i=0}^{p} \Big(L_i \cap Q_{k-2}(a) \Big) \setminus Q_{k-1}(a).$$

Then $L_i \cap X \cap Y = \varnothing$ for $i = 1, \ldots, p$, and $L_0 \cap X \cap Y = p-1$. Hence

$$\langle f, \mathbf{1}_X \rangle = |X \cap Y| = p - 1 \neq 0 \bmod p.$$

One can use (9.7) to construct similar examples in higher dimensions. For instance, the same argument would apply to a function $F(x_1, \ldots, x_n) = f(x_1, x_2)$ on R^n, where f is as in (9.7). Further examples could be constructed by changing variables via nonsingular (mod p) linear mappings. However, we should point out that a function in $\mathcal{H}^n$ could have a phi function expansion where some of the phi functions appearing with nonzero coefficients are not, by themselves, in $\mathcal{H}^n$. As an example, we invite the reader to verify that the function $\phi_{12} + \phi_{21} : (\mathbb{Z}/4\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z}$ is in fact a hyperplane function.

9.5. Nearly-parallel lines

Any hyperplane H in R^n has the following property. Let Q be a cube on some scale ℓ, and let L, L' be two parallel lines in R^n, both passing through Q and making an angle $\angle(L, L') \leqslant p^{-1}$. Then

$$|L \cap Q \cap H| \equiv |L' \cap Q \cap H| \mod p.$$

We prove in Proposition 9.3 that a similar property holds for phi functions of degree at most $p^k - 1$.

Proposition 9.3. *Let Q be a cube on scale ℓ for some $0 \leqslant \ell \leqslant k-1$. Let L, L' be two lines in R^n. Assume that both L and L' pass through Q, and that $\angle(L, L') \leqslant p^{-1}$. Then for any function $f \in \Omega^n_{p^k-1}$ we have*

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

Proof. We prove the proposition under the assumption that $Q = R^n$. The general case can be deduced from this by rescaling as in Section 9.3. The details are left to the interested reader.

We first claim that it suffices to consider the case when L is a line in the direction of $e_1 = (1, 0, \ldots, 0)$. Indeed, let $b \in \mathbb{P}R^{n-1}$ be the direction vector for L. Without loss of

generality, we may assume that $b_1 \in R^\times$. Define a linear mapping $U : R^n \to R^n$ by saying that $U(e_1) = b$ and (with the obvious notation) $U(e_j) = e_j$ for $2 \leqslant j \leqslant n$. 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 4.6, $f(x)$ and $f(Ux)$ have the same degree. This proves the claim.

It therefore suffices to prove the following. Let L be a line in the direction of e_1, and let L' be a line making an angle at most p^{-1} with L. Then for any α with $|\alpha| \leqslant p^k - 1$ we have

$$\langle \mathbf{1}_L, \phi_\alpha \rangle \equiv \langle \mathbf{1}_{L'}, \phi_\alpha \rangle \mod p. \tag{9.8}$$

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

$$\langle \mathbf{1}_L, \phi_\alpha \rangle = \left(\sum_{y \in R} \phi_\beta(y) \right) \phi_\gamma(z).$$

If $0 \leqslant \beta < p^k - 1$, then by (3.3),

$$\sum_{y \in R} \phi_\beta(y) = \sum_{y \in R} (\phi_{\beta+1}(y+1) - \phi_{\beta+1}(y)) = 0. \tag{9.9}$$

Suppose now that $\beta = p^k - 1$. Since $\beta + |\gamma| = |\alpha| \leqslant p^k - 1$, it follows that $|\gamma| = 0$, so that $\phi_\gamma(z) = 1$. But then ϕ_α is the indicator function of the hyperplane $x_1 = p^k - 1$.

Similarly, we may write L' as $\{(y, z + pvy) : y \in R\}$ for some $z, v \in R^{n-1}$. Then

$$\begin{aligned} \langle \mathbf{1}_L, \phi_\alpha \rangle &= \sum_{y \in R} \phi_\beta(y) \phi_\gamma(z + pvy) \\ &= \sum_{y \in R} \sum_{\gamma' + \gamma'' = \gamma} \phi_\beta(y) \phi_{\gamma'}(z) \phi_{\gamma''}(pvy) \\ &= \sum_{y \in R} \sum_{\gamma' + p\nu = \gamma} \phi_\beta(y) \phi_{\gamma'}(z) \phi_\nu(vy), \end{aligned}$$

by the obvious extensions of (3.5) and (3.6) to multiindices. We expand each function $\phi_\beta(y)\phi_\nu(vy)$ in terms of $\phi_j(y)$ with $j \leqslant \beta + |\nu|$. By (9.9), each such term will sum to 0 in y unless $j = p^k - 1$. Since $\beta + p|\nu| \leqslant |\alpha| \leqslant p^k - 1$, the only way we can get a contributing term with $j = p^k - 1$ is when $\nu = 0 = \gamma$ and $\beta = p^k - 1$. As above, this implies that ϕ_α is the indicator function of the hyperplane $x_1 = p^k - 1$.

We now conclude the proof as follows. 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 (9.8) is clearly true. On the other hand, if at least one of the above is nonzero mod p, then ϕ_α is the indicator function of the hyperplane $x_1 = p^k - 1$. But in that case, (9.8) is again true with both sides equal to 1. This proves the proposition. □

Acknowledgements

We are very grateful to the anonymous referees for many helpful suggestions and especially for pointing us to important references on the subject.

References

[AM21] Erhard Aichinger and Jakob Moosbauer. Chevalley-Warning type results on abelian groups. *J. Algebra*, 569:30–66, 2021. doi:10.1016/j.jalgebra.2020.10.033.

[Ars21] Bodan Arsovski. The p-adic Kakeya conjecture. 2021. arXiv:2108.03750v1.

[Ars24] Bodan Arsovski. The p-adic Kakeya conjecture. *J. Amer. Math. Soc.*, 37(1):69–80, 2024. doi:10.1090/jams/1021.

[BCC+17] Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans. On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Anal.*, 3, 2017. doi:10.19086/da.1245.

[Car18] Xavier Caruso. Almost all non-archimedean Kakeya sets have measure zero. *Conflu. Math.*, 10(1):3–40, 2018. doi:10.5802/cml.44.

[CS22] Pete L. Clark and Uwe Schauz. Functional degrees and arithmetic applications I: the set of functional degrees. *J. Algebra*, 608:691–718, 2022. doi:10.1016/j.jalgebra.2022.05.035.

[CS23] Pete L. Clark and Uwe Schauz. Functional degrees and arithmetic applications II: The group-theoretic Ax-Katz Theorem. 2023. arXiv:2305.01304.

[DD21] Manik Dhar and Zeev Dvir. Proof of the Kakeya set conjecture over rings of integers modulo square-free N. *Comb. Theory*, 1:4, 2021. doi:10.5070/C61055361.

[DGY11] Zeev Dvir, Parikshit Gopalan, and Sergey Yekhanin. Matching vector codes. *SIAM J. Comput.*, 40(4):1154–1178, 2011. doi:10.1137/100804322.

[Dha22] Manik Dhar. Maximal and (m, ϵ)-Kakeya bounds over $\mathbb{Z}/N\mathbb{Z}$ for general N. 2022. arXiv:2209.11443.

[Dha23a] Manik Dhar. *Beyond the polynomial method: Kakeya sets over finite rings and high dimensional variants*. Phd thesis, Princeton University, Princeton, NJ, Sept 2023. Available at http://arks.princeton.edu/ark:/88435/dsp01xd07gw99z.

[Dha23b] Manik Dhar. (n, k)-Besicovitch sets do not exist in $\mathbb{Z}_p^n$ and $\hat{\mathbb{Z}}^n$ for $k \geqslant 2$. 2023. arXiv:2312.02495.

[Dha24] Manik Dhar. The Kakeya set conjecture over $\mathbb{Z}/N\mathbb{Z}$ for general N. *Adv. Comb.*, 2, 2024. doi:10.19086/aic.2024.2.

[Dvi09] Zeev Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009. doi:10.1090/S0894-0347-08-00607-3.

[EG17] Jordan S. Ellenberg and Dion Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Ann. Math.*, 185(1):339–343, 2017. doi:10.4007/annals.2017.185.1.8.

[Fré09] Maurice Fréchet. Une définition fonctionnelle des polynomes. *Nouv. Ann. Math.: J. Cand. Éc. Polytech. Norm.*, 9:145–162, 1909. URL: http://eudml.org/doc/102345.

[GD68] J. M. Goethals and P. Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Trans. Inf. Theory*, 14(2):182–188, 1968. doi:10.1109/TIT.1968.1054126.

[HW18] Jonathan Hickman and James Wright. The Fourier restriction and Kakeya problems over rings of integers modulo N. *Discrete Anal.*, 2018(11), 2018. doi:10.19086/da.3682.

[Kem21] Aubrey J. Kempner. Polynomials and their residue systems. *Trans. Amer. Math. Soc.*, 22(2):240–266, 1921. doi:10.2307/1989020.

[Lac04] M. Laczkovich. Polynomial mappings on abelian groups. *Aequationes Math.*, 68(3):177–199, 2004. doi:10.1007/s00010-004-2727-9.

[Lei02] A. Leibman. Polynomial mappings of groups. *Israel J. Math.*, 129:29–60, 2002. doi:10.1007/BF02773152.

[Li05] Shujun Li. Null polynomials modulo *m*. 2005. arXiv:math/0510217.

[Luc78] Edouard Lucas. Théorie des Fonctions Numériques Simplement Périodiques. [Continued]. *Amer. J. Math.*, 1(3):197–240, 1878. doi:10.2307/2369311.

[MM68] F. J. MacWilliams and H. B. Mann. On the p-rank of the design matrix of a difference set. *Inf. Control.*, 12(5):474–488, 1968. doi:10.1016/S0019-9958(68)90534-2.

[Pet16] Fedor Petrov. Combinatorial results implied by many zero divisors in a group ring. 2016. arXiv:1606.03256.

[Sch14] Uwe Schauz. Classification of polynomial mappings between commutative groups. *J. Number Theory*, 139:1–28, 2014. doi:10.1016/j.jnt.2013.12.010.

[Smi69] 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(2):122–129, 1969. doi:10.1016/S0021-9800(69)80046-3.

[Spe16] David Speyer. Bounds for sum free sets in prime power cyclic groups — three ways, 2016. Accessed June 2023. URL: https://sbseminar.wordpress.com/2016/07/08/bounds-for-sum-free-sets-in-prime-power-cyclic-groups-three-ways/.

[Wil06] Richard M. Wilson. A lemma on polynomials modulo p^m and applications to coding theory. *Discrete Math.*, 306(23):3154–3165, 2006. doi:10.1016/j.disc.2004.10.030.

[YGK12] Chen Yuan, Qian Guo, and Haibin Kan. A novel elementary construction of matching vectors. *Inf. Process. Lett.*, 112(12):494–496, 2012. doi:10.1016/j.ipl.2012.03.008.