

Bounds on Degrees of p -Adic Separating Polynomials.

Daniel J. Katz*

Joshua Zahl†

28 May 2007

Abstract

We study a discrete optimization problem introduced by Babai, Frankl, Kutin, and Štefankovič (2001), which provides bounds on degrees of polynomials with p -adically controlled behavior. Such polynomials are of particular interest because they furnish bounds on the size of set systems satisfying Frankl–Wilson-type conditions modulo prime powers, with lower degree polynomials providing better bounds. We elucidate the asymptotic structure of solutions to the optimization problem, and we also provide an improved method for finding solutions in certain circumstances.

1 Introduction

This note examines the function $D(s, k)$ defined by Babai, Frankl, Kutin, and Štefankovič [1] as

$$D(s, k) = \max_{p, B, a} \min_f \deg f,$$

where p runs over the primes, B can be any union of s cosets of the additive subgroup $p^k\mathbb{Z}$ of \mathbb{Z} , a runs through $\mathbb{Z} \setminus B$, and f runs through the polynomials in $\mathbb{Q}[x]$ that p -adically separate a from B , i.e., polynomials with the property that $v_p(f(a)) < v_p(f(b))$ for all $b \in B$, where $v_p(b)$ is the p -adic valuation of b . $D(s, k)$ is employed in [1] to obtain bounds on the size of set systems which satisfy Frankl–Wilson-type conditions modulo prime powers, i.e., families of subsets of $\{1, 2, \dots, n\}$ wherein the cardinalities of pairwise intersections in the family are all congruent to s residues modulo p^k and the cardinalities of the subsets themselves are incongruent to these s residues modulo p^k . The authors of [1], following the method of [2], show that that a polynomial in n of degree $D(s, k)$ is an upper bound on the number of subsets in any such family. Furthermore, [1] develops tight log-asymptotic bounds on $D(s, k)$ in terms of s and k .

In this note, we analyze the structure of $D(s, k)$ and shed some light on an open problem posed in [1] by finding a method for computing $D(s, k)$ which is especially efficient when s is very large compared to k . In Sections 2 and 3, we establish notations and formulate $D(s, k)$ as the maximum value of a discrete multi-variable function. Section 4 culminates in Proposition 4, which greatly narrows the domain over which we need to search for this maximum. Then in Section 5, we prove the main result of this note, Theorem 9, which shows that $D(s, k)$ is asymptotically a quasi-polynomial in s whose leading term is invariably $\frac{s^k}{k^k k!}$. Section 6 closes with a brief commentary on how the results of this paper can be used to simplify the calculation of $D(s, k)$.

*D. J. Katz was with the Department of Mathematics, California Institute of Technology, Pasadena, CA 91125 USA. He is now with the Department of Mathematics, Princeton University, Princeton, NJ 08544 USA (email: dankatz@math.princeton.edu)

†J. Zahl is at the California Institute of Technology, Pasadena, CA 91125 USA (email: jzahl@zahl.ca). Work supported by the Edward R. Roney summer undergraduate research fellowship.

2 Notation

Throughout this work, \mathbb{N} will denote the nonnegative integers and k a positive integer. Boldface letters \mathbf{a} will denote k -tuples (a_1, \dots, a_k) unless noted otherwise. For $m < n$, we identify the m -tuple (a_1, \dots, a_m) with the n -tuple $(a_1, \dots, a_m, 0, 0, \dots, 0)$.

An m -tuple $\mathbf{a} = (a_1, \dots, a_m)$ in $\{0, 1\}^m$ is identified with the set $\{z \in \{1, 2, \dots, m\} : a_z = 1\}$. Thus $\min \mathbf{a}$ is the lowest i such that $a_i = 1$ and $\max \mathbf{a}$ is the highest j such that $a_j = 1$. Under this identification, $\emptyset = (0, \dots, 0)$, which is also denoted by $\mathbf{0}$. Similarly, the k -tuple $(1, \dots, 1)$ is identified with $\{1, 2, \dots, k\}$, which shall also be denoted by $\mathbf{1}$. In the same manner, $\{j\} = (0, \dots, 0, 1, 0, \dots, 0)$, the k -tuple whose j th entry is 1 and whose other entries are all zero.

The *weight* of an m -tuple $\mathbf{a} \in \mathbb{Q}^m$ is $a_1 + \dots + a_m$, and is denoted briefly by $|\mathbf{a}|$. For tuples $\mathbf{a} \in \{0, 1\}^m$, our identification of tuples with sets makes $|\mathbf{a}|$ the cardinality of the set \mathbf{a} . If \mathbf{i} is a k -tuple of integers, then $\mathbf{s}^{\mathbf{i}}$ is shorthand for $s_1^{i_1} s_2^{i_2} \dots s_k^{i_k}$.

3 Definitions

In [1], it is shown that $D(s, k)$ is equal to the solution of a discrete optimization problem. We shall work with this alternative definition of $D(s, k)$, which we shall develop in this section.

For $\mathbf{s} \in \mathbb{Q}^k$ and $1 \leq j \leq k$, we recursively define

$$\ell_j(\mathbf{s}) = 1 + \left\lfloor \sum_{i=1}^{j-1} \ell_i(\mathbf{s}) s_i \left(1 - \frac{i}{j}\right) \right\rfloor. \quad (1)$$

For $\mathbf{r}, \mathbf{s} \in \mathbb{Q}^k$ and $1 \leq j \leq k$, we recursively define

$$\ell_j(\mathbf{r}, \mathbf{s}) = r_j + \sum_{i=1}^{j-1} \ell_i(\mathbf{r}, \mathbf{s}) s_i \left(1 - \frac{i}{j}\right). \quad (2)$$

Furthermore, we define

$$q_j(\mathbf{s}) = \left\lfloor \sum_{i=1}^{j-1} \ell_i(\mathbf{s}) s_i \left(1 - \frac{i}{j}\right) \right\rfloor + 1 - \sum_{i=1}^{j-1} \ell_i(\mathbf{s}) s_i \left(1 - \frac{i}{j}\right), \quad (3)$$

which is in $\left\{\frac{1}{j}, \dots, \frac{j}{j}\right\}$ if $\mathbf{s} \in \mathbb{Z}^k$, and note that

$$\ell_j(\mathbf{s}) = \ell_j(\mathbf{q}(\mathbf{s}), \mathbf{s}) \quad (4)$$

for all j . We also define

$$L(\mathbf{s}) = \sum_{i=1}^k \ell_i(\mathbf{s}) s_i,$$

and

$$L(\mathbf{r}, \mathbf{s}) = \sum_{i=1}^k \ell_i(\mathbf{r}, \mathbf{s}) s_i, \quad (5)$$

so we have

$$L(\mathbf{s}) = L(\mathbf{q}(\mathbf{s}), \mathbf{s}). \quad (6)$$

For $s \in \mathbb{N}$, we define

$$D(s, k) = \max_{\mathbf{s} \in \mathbb{N}^k, |\mathbf{s}|=s} L(\mathbf{s}),$$

and we note that this definition coincides with Definition 2.3 of [1].

4 Uniformity Results

In Proposition 4 of this section, we prove that maximizers of $L(\mathbf{s})$ are asymptotically uniform, in particular, that a maximizer $\mathbf{s} = (s_1, \dots, s_k)$ has $|s_x - s_y| < 2k!$ for all x, y . This result is based on a careful analysis of the structure of $L(\mathbf{s})$ in the following three lemmas.

Lemma 1. *Suppose that $\mathbf{r} \in \mathbb{Q}^k$. For each $\mathbf{i} \in \{0, 1\}^k$, suppose that $j_1 < j_2 < \dots < j_t$ are the elements of the set with which \mathbf{i} is identified, and define*

$$c_{\mathbf{i}} = \left(1 - \frac{j_1}{j_2}\right) \left(1 - \frac{j_2}{j_3}\right) \dots \left(1 - \frac{j_{t-1}}{j_t}\right), \quad (7)$$

where the product is interpreted as 1 if \mathbf{i} is a singleton set or the empty set. Then

$$L(\mathbf{r}, \mathbf{s}) = \sum_{\substack{\mathbf{i} \in \{0, 1\}^k \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}}.$$

Proof. In view of (5) and since

$$\left\{ \mathbf{i} \in \{0, 1\}^k : \mathbf{i} \neq \emptyset \right\} = \bigsqcup_{t=1}^k \left\{ \mathbf{i} \in \{0, 1\}^t : i_t = 1 \right\},$$

with our identification of tuples of different lengths specified above, it suffices to prove that

$$s_t \ell_t(\mathbf{r}, \mathbf{s}) = \sum_{\substack{\mathbf{i} \in \{0, 1\}^t \\ i_t = 1}} c_{\mathbf{i}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}},$$

which will follow from

$$\ell_t(\mathbf{r}, \mathbf{s}) = r_t + \sum_{\substack{\mathbf{i} \in \{0, 1\}^{t-1} \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i} + \{t\}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}} \quad (8)$$

if we multiply by s_t and re-index. We prove (8) by induction on t .

The $t = 1$ case is transparent, since the sum becomes empty. We expand out the definition (1) of $\ell_t(\mathbf{r}, \mathbf{s})$ using the induction hypothesis:

$$\begin{aligned} \ell_t(\mathbf{r}, \mathbf{s}) &= r_t + \sum_{j=1}^{t-1} s_j \left(r_j + \sum_{\substack{\mathbf{i} \in \{0, 1\}^{j-1} \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i} + \{j\}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}} \right) \left(1 - \frac{j}{t}\right) \\ &= r_t + \sum_{j=1}^{t-1} \left(1 - \frac{j}{t}\right) s_j r_j + \sum_{j=1}^{t-1} \sum_{\substack{\mathbf{i} \in \{0, 1\}^{j-1} \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i} + \{j\}} \left(1 - \frac{j}{t}\right) \mathbf{s}^{\mathbf{i} + \{j\}} r_{\min \mathbf{i}}. \end{aligned}$$

For each value of j in the outer sum of the double sum, the tuple $\mathbf{i} + \{j\}$ occurring within the inner sum runs over all j -tuples of weight greater than one with k th coordinate equal to 1. When we

identify all these with $(t-1)$ -tuples in the usual way, we get all the $(t-1)$ -tuples of weight greater than 1, so

$$\begin{aligned}
\ell_t(\mathbf{r}, \mathbf{s}) &= r_t + \sum_{j=1}^{t-1} \left(1 - \frac{j}{t}\right) s_j r_j + \sum_{\substack{\mathbf{i} \in \{0,1\}^{t-1} \\ |\mathbf{i}| > 1}} c_{\mathbf{i}} \left(1 - \frac{\max \mathbf{i}}{t}\right) \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}} \\
&= r_t + \sum_{\substack{\mathbf{i} \in \{0,1\}^{t-1} \\ |\mathbf{i}| = 1}} c_{\mathbf{i}} \left(1 - \frac{\max \mathbf{i}}{t}\right) \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}} + \sum_{\substack{\mathbf{i} \in \{0,1\}^{t-1} \\ |\mathbf{i}| > 1}} c_{\mathbf{i}} \left(1 - \frac{\max \mathbf{i}}{t}\right) \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}} \\
&= r_t + \sum_{\substack{\mathbf{i} \in \{0,1\}^{t-1} \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i}} \left(1 - \frac{\max \mathbf{i}}{t}\right) \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}}.
\end{aligned}$$

Now note that $c_{\mathbf{i}} \left(1 - \frac{\max \mathbf{i}}{t}\right)$ in the last sum is the same as $c_{\mathbf{i}+\{t\}}$, so that (8) is proved. \square

Lemma 2. *Let $k \geq 2$, and let the coefficients $c_{\mathbf{i}}$ be as defined in Lemma 1. Suppose that $\mathbf{i} \in \{0,1\}^k$ with $\mathbf{i} \neq \emptyset$, and that $j \in \{1, 2, \dots, k\}$ with $i_j = 0$. Then $c_{\mathbf{i}+\{j\}} \geq \frac{c_{\mathbf{i}}}{2(k-1)}$ and furthermore, if $j > \max \mathbf{i}$ or $j < \min \mathbf{i}$, then $c_{\mathbf{i}+\{j\}} \geq \frac{c_{\mathbf{i}}}{k}$.*

Proof. If $j < \min \mathbf{i}$, then

$$c_{\mathbf{i}+\{j\}} = \left(1 - \frac{j}{\min \mathbf{i}}\right) c_{\mathbf{i}} \geq \frac{c_{\mathbf{i}}}{k},$$

and similarly, if $j > \max \mathbf{i}$, then

$$c_{\mathbf{i}+\{j\}} = \left(1 - \frac{\max \mathbf{i}}{j}\right) c_{\mathbf{i}} \geq \frac{c_{\mathbf{i}}}{k}.$$

If $i_s = i_t = 1$ for $s < t$ with $i_{s+1} = i_{s+2} = \dots = i_{t-1} = 0$ and $s < j < t$, then

$$c_{\mathbf{i}+\{j\}} = \frac{\left(1 - \frac{s}{j}\right) \left(1 - \frac{j}{t}\right)}{1 - \frac{s}{t}} c_{\mathbf{i}} = \frac{\left(1 - \frac{s}{j}\right) \left(\frac{t}{j} - 1\right)}{\frac{t}{j} - \frac{s}{j}} c_{\mathbf{i}}. \quad (9)$$

Now

$$\frac{(1-x)(y-1)}{y-x} = (y-1) - \frac{(y-1)^2}{y-x} = (1-x) - \frac{(1-x)^2}{y-x}$$

is decreasing in x and increasing in y , so the fraction in (9) is minimized when $\frac{s}{j}$ is maximized and when $\frac{t}{j}$ is minimized. For any given value of j , this occurs when $s = j-1$ and $t = j+1$. Substituting these two values into the above equation and noting that $j < t \leq k$ yields the desired inequality

$$c_{\mathbf{i}+\{j\}} \geq \frac{c_{\mathbf{i}}}{2(k-1)}. \quad \square$$

Lemma 3. *If $\mathbf{s} \in \mathbb{Z}^k$, and $1 \leq j \leq k$, then $q_i(\mathbf{s} + k!\{j\}) = q_i(\mathbf{s})$ and $\ell_i(\mathbf{s} + k!\{j\}) \equiv \ell_i(\mathbf{s}) \pmod{\frac{k!}{i!}}$ for all $i \in \{1, 2, \dots, k\}$.*

Proof. Let $\mathbf{t} = \mathbf{s} + k!\{j\}$; we will prove by induction on i that $q_i(\mathbf{t}) = q_i(\mathbf{s})$ and $\ell_i(\mathbf{t}) \equiv \ell_i(\mathbf{s}) \pmod{\frac{k!}{i!}}$ for all $i \in \{1, 2, \dots, k\}$. The conclusions clearly follow for all $i \leq j$ since $q_i(\mathbf{s})$ and $\ell_i(\mathbf{s})$ do not depend on the j th coordinate of \mathbf{s} when $i \leq j$.

Assume that $i > j$ and that $q_h(\mathbf{t}) = q_h(\mathbf{s})$ and $\ell_h(\mathbf{t}) \equiv \ell_h(\mathbf{s}) \pmod{\frac{k!}{h!}}$ for all $h < i$. Examining (3), we can see that $q_i(\mathbf{s})$ is determined solely by the residues of $1s_1\ell_1(\mathbf{s}), 2s_2\ell_2(\mathbf{s}), \dots, (i-1)s_{i-1}\ell_{i-1}(\mathbf{s})$ modulo i , and similarly for $q_i(\mathbf{t})$. However, by our induction hypothesis and the fact that $\mathbf{t} = \mathbf{s} + k!\{j\}$, we have $1s_1\ell_1(\mathbf{s}) \equiv 1t_1\ell_1(\mathbf{t}), \dots, (i-1)s_{i-1}\ell_{i-1}(\mathbf{s}) \equiv (i-1)t_{i-1}\ell_{i-1}(\mathbf{t})$ modulo i , so we have $q_i(\mathbf{s}) = q_i(\mathbf{t})$.

Since

$$\ell_i(\mathbf{s}) = q_i(\mathbf{s}) + \sum_{h=1}^{i-1} \ell_h(\mathbf{s})s_h \left(1 - \frac{h}{i}\right),$$

and

$$\ell_i(\mathbf{t}) = q_i(\mathbf{t}) + \sum_{h=1}^{i-1} \ell_h(\mathbf{t})t_h \left(1 - \frac{h}{i}\right),$$

by (4) and (2), the fact that $\ell_h(\mathbf{t}) \equiv \ell_h(\mathbf{s}) \pmod{\frac{k!}{h!}}$ for all $h < i$, along with $q_i(\mathbf{t}) = q_i(\mathbf{s})$ and $\mathbf{t} = \mathbf{s} + k!\{j\}$, also shows us that $\ell_i(\mathbf{t}) \equiv \ell_i(\mathbf{s}) \pmod{\frac{k!}{i!}}$. \square

Proposition 4. *Suppose that $\mathbf{s} \in \mathbb{N}^k$ and $1 \leq x, y \leq k$ such that $s_y - s_x \geq 2k!$. Then*

$$L(\mathbf{s} + k!\{x\} - k!\{y\}) > L(\mathbf{s}).$$

Proof. We assume $k \geq 2$ henceforth, since the hypotheses cannot be fulfilled otherwise. Let $\mathbf{t} = \mathbf{s} + k!\{x\} - k!\{y\}$. We shall to show that $L(\mathbf{t}) > L(\mathbf{s})$, or equivalently by (6), that $L(\mathbf{q}(\mathbf{t}), \mathbf{t}) > L(\mathbf{q}(\mathbf{s}), \mathbf{s})$. By Lemma 3, $\mathbf{q}(\mathbf{t}) = \mathbf{q}(\mathbf{s})$. Denote this k -tuple by \mathbf{r} , which satisfies $\frac{1}{j} \leq r_j \leq 1$ for all j . Thus it is sufficient to show that $L(\mathbf{r}, \mathbf{t}) > L(\mathbf{r}, \mathbf{s})$. By Lemma 1, this amounts to showing that

$$\sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i}} \mathbf{t}^{\mathbf{i}} r_{\min \mathbf{i}} > \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}},$$

where the coefficients $c_{\mathbf{i}}$ are the positive rationals as defined in that lemma. If \mathbf{i} has $i_x = i_y = 0$, then $\mathbf{t}^{\mathbf{i}} = \mathbf{s}^{\mathbf{i}}$, and if \mathbf{i} has $i_x = 1$ and $i_y = 0$, then $\mathbf{t}^{\mathbf{i}} \geq \mathbf{s}^{\mathbf{i}}$, with equality only if $s_j = 0$ for some $j \neq x$ such that $i_j = 1$. In particular $\mathbf{t}^{\{x\}} = t_x > s_x = \mathbf{s}^{\{x\}}$. Thus

$$\sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset, i_y=0}} c_{\mathbf{i}} \mathbf{t}^{\mathbf{i}} r_{\min \mathbf{i}} > \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset, i_y=0}} c_{\mathbf{i}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}},$$

and so it suffices for us to show that

$$\sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ i_y=1}} c_{\mathbf{i}} \mathbf{t}^{\mathbf{i}} r_{\min \mathbf{i}} \geq \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ i_y=1}} c_{\mathbf{i}} \mathbf{s}^{\mathbf{i}} r_{\min \mathbf{i}},$$

or equivalently, that

$$\sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ i_x=i_y=1}} c_{\mathbf{i}} (\mathbf{t}^{\mathbf{i}} - \mathbf{s}^{\mathbf{i}}) r_{\min \mathbf{i}} \geq \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ i_x=0, i_y=1}} c_{\mathbf{i}} (\mathbf{s}^{\mathbf{i}} - \mathbf{t}^{\mathbf{i}}) r_{\min \mathbf{i}},$$

which we shall show by showing that for any $\mathbf{i} \in \{0,1\}^k$ with $i_x = i_y = 0$, we have

$$c_{\mathbf{i}+\{x,y\}} (\mathbf{t}^{\mathbf{i}+\{x,y\}} - \mathbf{s}^{\mathbf{i}+\{x,y\}}) r_{\min(\mathbf{i}+\{x,y\})} \geq c_{\mathbf{i}+\{y\}} (\mathbf{s}^{\mathbf{i}+\{y\}} - \mathbf{t}^{\mathbf{i}+\{y\}}) r_{\min(\mathbf{i}+\{y\})}.$$

The last inequality is equivalent to

$$c_{\mathbf{i}+\{x,y\}} \mathbf{s}^{\mathbf{i}} [(s_x + k!)(s_y - k!) - s_x s_y] r_{\min(\mathbf{i}+\{x,y\})} \geq c_{\mathbf{i}+\{y\}} \mathbf{s}^{\mathbf{i}} [s_y - (s_y - k!)] r_{\min(\mathbf{i}+\{y\})},$$

which in turn is equivalent to

$$[k!(s_y - s_x) - (k!)^2] c_{\mathbf{i}+\{x,y\}} \mathbf{s}^{\mathbf{i}} r_{\min(\mathbf{i}+\{x,y\})} \geq k! c_{\mathbf{i}+\{y\}} \mathbf{s}^{\mathbf{i}} r_{\min(\mathbf{i}+\{y\})}.$$

Since $s_y - s_x \geq 2k!$ by hypothesis, it will suffice to show that

$$k! c_{\mathbf{i}+\{x,y\}} r_{\min(\mathbf{i}+\{x,y\})} \geq c_{\mathbf{i}+\{y\}} r_{\min(\mathbf{i}+\{y\})}. \quad (10)$$

If $x < \min(\mathbf{i} + \{y\})$, then by Lemma 2, we know that $c_{\mathbf{i}+\{x,y\}} \geq \frac{c_{\mathbf{i}+\{y\}}}{k}$, so it will suffice to show that

$$(k-1)! r_{\min(\mathbf{i}+\{x,y\})} \geq r_{\min(\mathbf{i}+\{y\})}.$$

Since $r_{\min(\mathbf{i}+\{x,y\})} \geq \frac{1}{x}$ and $r_{\min(\mathbf{i}+\{y\})} \leq 1$, it suffices to show that $(k-1)! \geq x$, which follows because $x < \min(\mathbf{i} + \{y\}) \leq k$. On the other hand, if $x > \min(\mathbf{i} + \{y\})$, then by Lemma 2, we know that $c_{\mathbf{i}+\{x,y\}} \geq \frac{c_{\mathbf{i}+\{y\}}}{2(k-1)}$, so to show (10), it suffices to show that

$$k! r_{\min(\mathbf{i}+\{x,y\})} \geq 2(k-1) r_{\min(\mathbf{i}+\{y\})},$$

and since $\min(\mathbf{i} + \{x,y\}) = \min(\mathbf{i} + \{y\})$, it suffices to show that $k! \geq 2(k-1)$, which is clearly true. \square

Corollary 5. *If $s \in \mathbb{N}$, $\mathbf{s} \in \mathbb{N}^k$ with $|\mathbf{s}| = s$, and $L(\mathbf{s}) = D(s, k)$, then $|s_x - \frac{s}{k}| < 2k!$ for all x .*

Proof. If for some x , $|s_x - \frac{s}{k}| \geq 2k!$, then there is some s_y such that $|s_x - s_y| > 2k!$, and we could use Proposition 4 to find some \mathbf{s}' with $L(\mathbf{s}') > L(\mathbf{s})$, so we cannot have $L(\mathbf{s}) = D(s, k)$. \square

Remark 6. By a more delicate analysis, we can prove the stronger result that if $|\mathbf{s}| = s$, $s \geq 8k^3 k!$, and $L(\mathbf{s}) = D(s, k)$, then $|s_x - s_y| < 4k$ for all x, y . Since this fact is not needed here, the proof has been omitted for brevity.

5 Asymptotic Form of $D(s, k)$

In Theorem 9, we prove that $D(s, k)$ asymptotically becomes equal to a quasi-polynomial. Some preliminary calculations needed to prove this are gathered in Lemma 7. Proposition 8 contains the main idea of the section: if \mathbf{s} is a k -tuple with $|\mathbf{s}| = s$ such that $D(s, k) = L(\mathbf{s})$ and s is sufficiently large, then $\mathbf{s} + k!\mathbf{1}$ will be a k -tuple with $|\mathbf{s} + k!\mathbf{1}| = s + kk!$ such that $D(s + kk!, k) = L(\mathbf{s} + k!\mathbf{1})$. This leads directly to the main result in Theorem 9.

Lemma 7. *Let $\mathbf{a} \in \mathbb{Z}^k$ and $B \in \mathbb{Q}$ with $|a_i| \leq B$ for all i . Then $g(u) = L(\mathbf{a} + uk!\mathbf{1})$ is a polynomial of degree k in $\mathbb{Q}[u]$ with $k!g(u) \in \mathbb{Z}[u]$. If we write $g(u) = g_0 + g_1 u + \cdots + g_k u^k$, then $g_k = (k!)^{k-1}$, and $|g_0| + |g_1| + \cdots + |g_k| \leq -1 + (k! + B + 1)^k$.*

Proof. By Lemma 3, we note that $\mathbf{q}(\mathbf{a} + uk!\mathbf{1}) = \mathbf{q}(\mathbf{a})$ for all $u \in \mathbb{N}$. Therefore, by (6) and Lemma 1, we have

$$\begin{aligned} g(u) &= L(\mathbf{a} + uk!\mathbf{1}) \\ &= L(\mathbf{a} + uk!\mathbf{1}, \mathbf{q}(\mathbf{a})) \\ &= \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} c_{\mathbf{i}}(\mathbf{a} + uk!\mathbf{1})^{\mathbf{i}} q_{\min \mathbf{i}}(\mathbf{a}), \end{aligned}$$

where c_i is as defined in Lemma 1. Thus $g(u)$ is a polynomial of degree k in $\mathbb{Q}[u]$ with leading coefficient $c_1(k!u)^k q_1(\mathbf{a})$. We can calculate that $c_1 = \frac{1}{k!}$ from the definition of c_i in Lemma 1, and can see from (3) that $q_1(\mathbf{a}) = 1$ for any $\mathbf{a} \in \mathbb{N}^k$. So the leading term of $g(u)$ is $(k!)^{k-1}u^k$. Recall that $q_j(\mathbf{a})$ is always an integer divided by j . From the definition of c_i in Lemma 1, it is then clear that $k!c_i q_{\min \mathbf{i}}(\mathbf{a})$ is an integer. So $k!g_{\mathbf{a}}(u) \in \mathbb{Z}[u]$.

Now we find an upper bound on the sum of the absolute values of the coefficients of $g(u)$. Since

$$g(u) = \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} c_i(\mathbf{a} + uk!\mathbf{1})^{\mathbf{i}} q_{\min \mathbf{i}}(\mathbf{a}),$$

for each $t \in \{0, 1, \dots, k\}$, the coefficient of u^t in $g(u)$ is

$$\sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} c_i q_{\min \mathbf{i}}(\mathbf{a}) \sum_{\substack{\mathbf{j} \in \{0,1\}^k \\ \mathbf{j} \subseteq \mathbf{i} \\ |\mathbf{j}| = |\mathbf{i}| - t}} \mathbf{a}^{\mathbf{j}} (k!)^t.$$

Since $c_i \leq 1$ for all \mathbf{i} (see the definition in Lemma 1), $q_i(\mathbf{a}) \leq 1$ for all i (see (3)), and $|a_i| \leq B$ for all i , the magnitude of the coefficient of u^t in $g(u)$ is at most

$$\begin{aligned} \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} \sum_{\substack{\mathbf{j} \in \{0,1\}^k \\ \mathbf{j} \subseteq \mathbf{i} \\ |\mathbf{j}| = |\mathbf{i}| - t}} B^{|\mathbf{j}|} (k!)^t &= \sum_{\substack{\mathbf{i} \in \{0,1\}^k \\ \mathbf{i} \neq \emptyset}} \binom{|\mathbf{i}|}{t} B^{|\mathbf{i}| - t} (k!)^t \\ &= \sum_{h=1}^k \binom{k}{h} \binom{h}{t} B^{h-t} (k!)^t. \end{aligned}$$

Thus the sum of the absolute values of the coefficients in $g_{\mathbf{a}}(u)$ is at most

$$\begin{aligned} \sum_{t=0}^k \sum_{h=1}^k \binom{k}{h} \binom{h}{t} B^{h-t} (k!)^t &= \sum_{h=1}^k \binom{k}{h} \sum_{t=0}^h \binom{h}{t} B^{h-t} (k!)^t \\ &= \sum_{h=1}^k \binom{k}{h} (k! + B)^h \\ &= -1 + (k! + B + 1)^k. \end{aligned} \quad \square$$

Proposition 8. *There exist $\mathbf{a}_0, \dots, \mathbf{a}_{kk!-1} \in \mathbb{N}^k$ with $|\mathbf{a}_\sigma| = \sigma$ for all σ such that if $s \geq \frac{k}{8}(4k!)^{k+2}$, then $D(s, k) = L(\mathbf{a}_{\bar{s}} + \frac{s-\bar{s}}{k}\mathbf{1})$, where \bar{s} is the reduction modulo $kk!$ of s .*

Proof. For each $\sigma \in \{0, 1, \dots, kk! - 1\}$, let $A(\sigma)$ denote the collection of $\mathbf{a} \in \mathbb{Z}^k$ with $|\mathbf{a}| = \sigma$ and $|a_i - a_j| < 2k!$ for all distinct i and j . Note that $A(\sigma)$ is finite and that if $\mathbf{a} \in A(\sigma)$ then $-2k! < a_i < 3k!$ for all i . For any $\sigma \in \{0, 1, \dots, kk! - 1\}$ and $u \geq 2$, let $B(\sigma, u) = \{\mathbf{a} + uk!\mathbf{1} : \mathbf{a} \in A(\sigma)\}$, which is precisely the subset of \mathbb{N}^k consisting of those \mathbf{s} with $|\mathbf{s}| = \sigma + ukk!$ and $|s_i - s_j| < 2k!$ for all distinct i, j . We have insisted upon $u \geq 2$ in the definition to insure that no k -tuple in $B(\sigma, u)$ has negative components. Proposition 4 implies that

$$\begin{aligned} D(\sigma + ukk!, k) &= \max_{\mathbf{s} \in B(\sigma, u)} L(\mathbf{s}) \\ &= \max_{\mathbf{a} \in A(\sigma)} L(\mathbf{a} + uk!\mathbf{1}) \end{aligned}$$

for $\sigma \in \{0, 1, \dots, kk! - 1\}$ and $u \geq 2$. For each $\mathbf{a} \in \mathbb{N}^k$, we define

$$g_{\mathbf{a}}(u) = L(\mathbf{a} + uk!\mathbf{1}), \quad (11)$$

which is a polynomial in $\mathbb{Q}[u]$ whose properties are detailed in Lemma 7, and for which

$$D(\sigma + ukk!, k) = \max_{\mathbf{a} \in A(\sigma)} g_{\mathbf{a}}(u)$$

for $\sigma \in \{0, 1, \dots, kk! - 1\}$ and $u \geq 2$.

Since $A(\sigma)$ is a finite collection of k -tuples, the corresponding collection $\{g_{\mathbf{a}} : \mathbf{a} \in A(\sigma)\}$ of polynomials is also finite, so there exists some $\mathbf{a}_{\sigma} \in A(\sigma)$ and $M_{\sigma} \in \mathbb{N}$ such that for all $\mathbf{a} \in A(\sigma)$, we have $g_{\mathbf{a}_{\sigma}}(u) \geq g_{\mathbf{a}}(u)$ for all $u \geq M_{\sigma}$, i.e., $g_{\mathbf{a}_{\sigma}}$ dominates all other polynomials in $\{g_{\mathbf{a}} : \mathbf{a} \in A(\sigma)\}$. Thus, for $u \geq M_{\sigma}$, $D(\sigma + ukk!, k) = g_{\mathbf{a}_{\sigma}}(u)$. Note that it is possible that two $\mathbf{a} \in A(\sigma)$ produce the same polynomial, so \mathbf{a}_{σ} may not be uniquely determined. Since there are only finitely many values of σ , there is a uniform bound M such that if $\sigma \in \{0, 1, \dots, kk! - 1\}$ and $u \geq M$, then $D(\sigma + ukk!, k) = g_{\mathbf{a}_{\sigma}}(u)$. So if $s \geq kk!M$, and if we use \bar{s} to denote the reduction modulo $kk!$ of s , then

$$D(s, k) = g_{\mathbf{a}_{\bar{s}}} \left(\frac{s - \bar{s}}{kk!} \right) = L \left(\mathbf{a}_{\bar{s}} + \frac{s - \bar{s}}{k} \mathbf{1} \right).$$

We will now find an explicit value of M (in terms of k) for which the above statement is true. Suppose that $\sigma \in \{0, 1, \dots, kk! - 1\}$, and recall that $\mathbf{a}_{\sigma} \in A(\sigma)$ is chosen so that $g_{\mathbf{a}_{\sigma}}(u)$ asymptotically dominates all other polynomials in $\{g_{\mathbf{a}} : \mathbf{a} \in A(\sigma)\}$. Let \mathbf{a} be any other element of $A(\sigma)$ such that $g_{\mathbf{a}}(u) \neq g_{\mathbf{a}_{\sigma}}(u)$. Let $h(u) = g_{\mathbf{a}_{\sigma}}(u) - g_{\mathbf{a}}(u)$, let d be the degree of $h(u)$, and write $h(u) = h_d u^d + \dots + h_1 u + h_0$. Clearly $h_d > 0$ because $g_{\mathbf{a}_{\sigma}}(u)$ eventually dominates $g_{\mathbf{a}}(u)$. For all $u \geq (|h_{d-1}| + \dots + |h_1| + |h_0|)/h_d$, we shall have $h(u) \geq 0$, i.e., $g_{\mathbf{a}_{\sigma}}(u) \geq g_{\mathbf{a}}(u)$. By Lemma 7, the sum of the magnitudes of the coefficients of $g_{\mathbf{a}}(u)$ is less than $(4k!)^k$ since $|a_i| < 3k!$ for all i . The same may be said of the coefficients of $g_{\mathbf{a}_{\sigma}}(u)$, so the sum of the magnitudes of the coefficients of $h(u)$ is less than $2(4k!)^k$. Lemma 7 also tells us that $k!g_{\mathbf{a}}(u)$ and $k!g_{\mathbf{a}_{\sigma}}(u)$ are in $\mathbb{Z}[u]$, so the leading coefficient of $h(u)$ is at least $\frac{1}{k!}$. Thus $(|h_{d-1}| + \dots + |h_1| + |h_0|)/h_d \leq 2k!(4k!)^k$. So if we set $M = \frac{1}{2}(4k!)^{k+1}$, we will have $g_{\mathbf{a}_{\sigma}}(u) - g_{\mathbf{a}}(u) = h(u) \geq 0$ for $u \geq M$. Thus for $s \geq kk!M = \frac{k}{8}(4k!)^{k+2}$, we have $D(s, k) = L(\mathbf{a}_{\bar{s}} + \frac{s - \bar{s}}{k} \mathbf{1})$. \square

Theorem 9. *There exist polynomials $f_0(s), \dots, f_{kk!-1}(s)$ in $\mathbb{Q}[s]$ such that $D(s, k) = f_{\bar{s}}(s)$ for all $s \geq \frac{k}{8}(4k!)^{k+2}$, where \bar{s} denotes the reduction modulo $kk!$ of s . Each $f_{\sigma}(s)$ has leading term $\frac{1}{k^k k!} s^k$, and if $k \geq 2$, the polynomials $f_0, \dots, f_{kk!-1}$ are not all identical.*

Proof. Let $\mathbf{a}_1, \dots, \mathbf{a}_{kk!-1}$ be as given by Proposition 8. For each $\sigma \in \{0, 1, \dots, kk! - 1\}$, we define $f_{\sigma}(s) = L(\mathbf{a}_{\sigma} + \frac{s - \sigma}{k} \mathbf{1})$, so that $D(s, k) = f_{\bar{s}}(s)$ for all $s \geq \frac{k}{8}(4k!)^{k+2}$. By Lemma 7, $L(\mathbf{a}_{\sigma} + uk!\mathbf{1})$ is a polynomial in $\mathbb{Q}[u]$ with leading term $(k!)^{k-1} u^k$, so $f_{\sigma}(s)$ is a polynomial in $\mathbb{Q}[s]$ with leading term $\frac{1}{k^k k!} s^k$.

Now suppose $k \geq 2$ and that $f_0(s), f_1(s), \dots, f_{kk!-1}(s)$ are identical in order to show a contradiction. In this case $D(s, k) = f_0(s)$ for $s \geq \frac{k}{8}(4k!)^{k+2}$. Write $f_0(s) = \sum_{i=0}^k c_k \binom{s}{i}$ where $\binom{s}{i}$ is the binomial coefficient polynomial $\frac{s(s-1)\dots(s-i+1)}{i!}$ (with $\binom{s}{0} = 1$). Let Δ be the finite difference operator, which takes a polynomial $f(s)$ to $f(s+1) - f(s)$. It is not hard to show that $\Delta \binom{s}{j} = \binom{s}{j-1}$ if $j > 0$, and that $\Delta \binom{s}{0} = 0$. Thus $c_k = (\Delta^k f_0)(s)$. Now $f_0(s) = D(s, k)$, so that $f_0(s)$ is integer-valued for integral $s \geq \frac{k}{8}(4k!)^{k+2}$, and so $(\Delta^k f_0)(s)$ must also be integer-valued for these s , i.e., c_k must be an integer. So the leading coefficient of $f_0(s)$ is $\frac{c_k}{k!}$ with c_k an integer, which contradicts the fact already established that the leading coefficient is $\frac{1}{k^k k!}$. \square

Remark 10. By carefully tracking the terms of degree s^{k-1} in the expansion of $L(\mathbf{a}_\sigma + \frac{s-\sigma}{k}\mathbf{1})$, it is possible to show that the next-to-leading term of each polynomial $f_\sigma(s)$ in the above theorem is $\frac{1}{k^{k-3}k!}s^{k-1}$ when $k \geq 2$. We omit the proof for brevity. Terms of degree $k-2$ may differ among $f_0(s), \dots, f_{kk!-1}(s)$, e.g., when $k = 2$, we have $f_0(s) = \frac{s^2}{8} + s$, $f_1(s) = f_3(s) = \frac{s^2}{8} + s - \frac{1}{8}$, and $f_2(s) = \frac{s^2}{8} + s - \frac{1}{2}$.

6 Computation of $D(s, k)$

By Corollary 5, if $\mathbf{s} \in \mathbb{N}$ with $s = |\mathbf{s}|$ and $L(\mathbf{s}) = D(s, k)$, then $|s_i - \frac{s}{k}| < 2k!$ for all i . Thus we can find those \mathbf{s} satisfying $L(\mathbf{s}) = D(s, k)$ by comparing the values of $L(\mathbf{s})$ for all $\mathbf{s} \in \mathbb{N}^k$ satisfying this uniformity condition. Our set of candidates contains at most $(4k!)^k$ elements, so this method will take at most $(4k!)^k$ computations of $L(\mathbf{s})$. For s large compared to k , this is significantly better than the exhaustive search method described in [1], which takes roughly $\binom{s+k}{k}$ computations of $L(\mathbf{s})$.

Acknowledgement

The authors wish to thank Richard M. Wilson for his helpful advice on this work and its presentation.

References

- [1] L. Babai, P. Frankl, S. Kutin, and D. Štefankovič. Set systems with restricted intersections modulo prime powers. *J. Combin. Theory Ser. A*, 95(1):39–73, 2001
- [2] L. Babai, H.S. Snevily, and R.M. Wilson. A new proof of several inequalities on codes and sets. *J. Combin. Theory Ser. A*, 71(1):146–153, 1995