ABSTRACT

THE HILBERT - KUNZ FUNCTION OF A DIAGONAL HYPERSURFACE

A Dissertation Presented to the Faculty of the
Graduate School of Arts and Sciences of
Brandeis University, Waltham, Massachusetts

by

Chungsim Han

The following algebraic problem arises in Iwasawa theory : let M be a finitely generated $\mathbf{Z}/p[[x_1, \ldots, x_s]]$ - module, I_n the ideal generated by $x_1^{p^n}, \ldots, x_s^{p^n}$, $M_n = M/I_nM$, and e_n the $\mathbf{Z}/p$ dimension of M_n. How does e_n grow with n? The function $n \mapsto e_n$ will be called the Hilbert - Kunz function of M.

Let a be the Krull dimension of M. Monsky has shown that if $a \geq 1$, $e_n = cp^{an} + O(p^{(a-1)n})$, where c is a positive real constant. When $a = 1$, he has the more precise result that c is an integer and the error term is not merely bounded but eventually periodic.

In this thesis, we study the case

$$M = F[[x_1, \cdots, x_s]]/(x_1^{d_1} + \cdots + x_s^{d_s})$$

where F is a field of characteristic p and $d_1, \ldots, d_s$ are positive integers. In other words, we study how

$$e_n = \dim_F F[[x_1, \ldots, x_s]]/(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^{p^n}, \ldots, x_s^{p^n})$$

varies with n for fixed p and $d_1, \ldots, d_s$.

The first main result is that when $s = 3$ or when $p = 2$, a certain function $D_F(k_1, \ldots, k_s)$ is "p - induced" and that in these cases c is rational and the error term is eventually periodic.

The second is that when $s > 3$, under the hypothesis that $D_F(k_1, \ldots, k_s)$ is p - induced, c is again rational and the error term Δ_n is $O(p^{(s-3)n})$. Furthermore there are integers λ and $l^{\#}$ with $\lambda \geq 1$ such that $\Delta_{n+\lambda} = l^{\#}\Delta_n$ for large enough n. (Shortly after we completed this thesis, Monsky used the result for $s = 3$ to show that D_F is p - induced for all s. The proof will be an appendix to this thesis. So our second result holds unconditionally.)

THE HILBERT - KUNZ FUNCTION OF A DIAGONAL HYPERSURFACE

A Dissertation

Presented to

The Faculty of the Graduate School of Arts and Sciences

Brandeis University

Department of Mathematics

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

by

Chungsim Han

February 1992

This dissertation, directed and approved by the candidate's Committee, has been accepted and approved by the Graduate Faculty of Brandeis University in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Dean, Graduate School of Arts
and Sciences

FEB - 1 1992

Dissertation Committee

Paul Monsky
Chair

Ira Gessel

Acknoledgements

I would like to express my deep gratitude to my advisor, Professor Paul Monsky, for his help, patience and constant encouragement through many years.

I am also grateful to Professors Hickey and Eisenbud for their help with computers and Professors Gessel and Stevens for their kind interest in my work.

I would like to thank all the friends, in particular Young Soon Lukoff and Stefano Brocco, who made life more pleasant and interesting.

This thesis is dedicated to my parents with my deepest gratitude, for everything.

To my parents

Table of Contents

0. Introduction 1

1. Elementary properties of D_F 4

2. Matrices of binomial coefficients and the calculation of $[k_1, k_2, k_3]_F$ 7

3. Matrices of multinomial coefficients and a functional equation for D_F 20

4. Definition and properties of l_F 25

5. Some p - multiplicativity results 29

6. The D_F - conjecture 36

7. Applications of the D_F - conjecture to Hilbert - Kunz functions 42

References 50

Appendix (Paul Monsky) 51

0. Introduction

The following algebraic problem arises in Iwasawa theory : let M be a finitely generated $\mathbf{Z}/p[[x_1, \ldots, x_s]]$ - module, I_n the ideal generated by $x_1^{p^n}, \ldots, x_s^{p^n}$, $M_n = M/I_nM$, and e_n the $\mathbf{Z}/p$ dimension of M_n. How does e_n grow with n? (Roughly speaking, these e_n occur as the ranks of the p - primary part of the ideal class group in the levels of a multiple $\mathbf{Z}_p$ - extension, where M is the Greenberg - Iwasawa module of the extension [2].)

The function $n \mapsto e_n$ will be called the Hilbert - Kunz function of M (this is a modification of the Hilbert - Samuel function, or Hilbert characteristic polynomial of M).

Let a be the Krull dimension of M. If $a = 0$, then for large n, $I_nM = (0)$ and the Hilbert - Kunz function is constant. In [1], Monsky has shown that if $a \geq 1$, $e_n = cp^{an} + O(p^{(a-1)n})$, where c is a positive real constant. When $a = s$, c is the $\mathbf{Z}/p[[x_1, \ldots, x_s]]$ - rank of M. When $a = 1$, he has the more precise result that c is an integer and the error term is not merely bounded but eventually periodic (i.e. periodic for large n). But when $a > 1$, it is not known whether c is always rational and the error term is a mystery.

In this thesis, we study the case

$$M = F[[x_1, \cdots, x_s]]/(x_1^{d_1} + \cdots + x_s^{d_s})$$

where F is a field of characteristic p and $d_1, \ldots, d_s$ are positive integers. In other words, we study how

$$e_n = \dim_F F[[x_1, \ldots, x_s]]/(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^{p^n}, \ldots, x_s^{p^n})$$

varies with n for fixed p and $d_1, \ldots, d_s$. (Monsky previously made an unpublished study of the case $s = 3$, $d_1 = d_2 = d_3$.)

The first main result is that when $s = 3$ or when $p = 2$, a certain function $D_F(k_1, \ldots, k_s)$ is "p - induced" and that in these cases c is rational and the error term is eventually periodic.

The second is that when $s > 3$, under the hypothesis that $D_F(k_1, \ldots, k_s)$ is p - induced, c is again rational and the error term Δ_n is $O(p^{(s-3)n})$. Furthermore there are integers λ and $l^{\#}$ with $\lambda \geq 1$ such that $\Delta_{n+\lambda} = l^{\#}\Delta_n$ for large enough n. (Shortly after we completed this thesis, Monsky used the result for $s = 3$ to show that D_F is p - induced for all s. The proof will be an appendix to this thesis. So our second result holds unconditionally. It follows for example that when $p = 3$, $s = 5$ and each $d_i = 2$, $e_n = \frac{23}{19}3^{4n} - \frac{4}{19}5^n$ for all n. Explicit formulas of this kind were completely unexpected.)

In chapter 1, we define $D_F(k_1, \ldots, k_s)$ to be the dimension of

$$F[x_1, \ldots, x_s]/(x_1 + \cdots + x_s, x_1^{k_1}, \ldots, x_s^{k_s})$$

and show that e_n can be written as a sum of values of D_F. We also develop some elementary properties of D_F.

Chapter 2 is devoted to the case $s = 3$. We introduce for k_1, k_2, k_3 satisfying the triangle inequalities a non-negative half-integer, $[k_1, k_2, k_3]_F$, which is related to D_F by

$$D_F(k_1, k_2, k_3) = \frac{2k_1k_2 + 2k_1k_3 + 2k_2k_3 - k_1^2 - k_2^2 - k_3^2}{4} + [k_1, k_2, k_3]_F^2.$$

We show that $[k_1, k_2, k_3]_F = 0$ if and only if $k_1 + k_2 + k_3$ is even and a certain square matrix of binomial coefficients has non-singular reduction modulo p. We write the exponent to which p appears in the determinant of this matrix as a sum of terms. We introduce a certain honeycomb of $\mathbf{R}^3$ by octahedra and tetrahedra, and show that the n^{th} term of the exponent is positive if $\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right)$ lies in an octahedral cell of the honeycomb and is zero otherwise. As a consequence, $[k_1, k_2, k_3]_F = 0$ if and only if no point $\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right)$, $n \geq 0$, is in an octahedral cell of the honeycomb ; this leads to a simple geometric description of $[k_1, k_2, k_3]_F$. At the end of the chapter, using the properties of $[k_1, k_2, k_3]_F$, we calculate c explicitly when $s = 3$ and show that it is rational.

In chapter 3, we study certain matrices of multinomial coefficients which correspond to the maps on the graded pieces of $F[x_1, \ldots, x_{s-1}]/(x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}})$ induced by multiplication by $(x_1 + \cdots + x_{s-1})^{k_s}$. By manipulating these matrices, we derive a functional equation for D_F : for q a power of p and $0 \leq k_i \leq q$,

$$D_F(k_1, \ldots, k_s) = D_F(k_1, \ldots, k_{s-2}, q - k_{s-1}, q - k_s) + (k_{s-1} + k_s - q)k_1 \cdots k_{s-2}.$$

In chapter 4, we define a new function l_F by

$$l_F(k_1, \ldots, k_s) = (-1)^{s+k_1+\cdots+k_s} \sum_{\epsilon \in \{0,1\}^s} (-1)^{\epsilon_1+\cdots+\epsilon_s} D_F(k_1 + \epsilon_1, \ldots, k_s + \epsilon_s).$$

The functional equation for D_F then gives a simple functional equation for l_F : for q a power of p and $0 \leq k_i \leq q-1$,

$$l_F(k_1, \ldots, k_s) = l_F(k_1, \ldots, k_{s-2}, q-1-k_{s-1}, q-1-k_s).$$

We also use the functional equation for D_F to show that $D_F(k_1, \ldots, k_s) - D_F(k_1 + 1, k_2, \ldots, k_s) - D_F(k_1, k_2+1, k_3, \ldots, k_s) + D_F(k_1+1, k_2+1, k_3, \ldots, k_s)$ lies between 0 and $k_4 \cdots k_s$, which gives a bound for l_F.

In chapter 5, we introduce the notion of p - multiplicativity, which is critical for the calculation of e_n. The remaining part of chapter 5 is devoted to showing that l_F is p - multiplicative when $s = 3$ or when $p = 2$. When $s = 3$, the proof is based on the geometric criterion for $[k_1, k_2, k_3]_F$ to be zero and the fact that $D_F(k_1, k_2, k_3) - D_F(k_1+1, k_2, k_3) - D_F(k_1, k_2+1, k_3) + D_F(k_1+1, k_2+1, k_3)$ can only take the values 0 or 1. When $p = 2$, the functional equation for l_F immediately gives the p - multiplicativity of l_F. In these cases, l_F is either 1 or 0.

In chapter 6, we translate the notion of p - multiplicativity of l_F into a property of D_F ; that of being p - induced. As the main part of this chapter, we show, using the properties of l_F derived in chapter 4, that D_F is p - induced if and only if D_F satisfies further functional equations (Φ_r), one for each vector $r = (r_1, \ldots, r_s)$ of non-negative integers. We then conjecture that D_F is p - induced for any fixed p and s, and give several cases in which this conjecture holds.

In the last chapter, we show that if D_F satisfies condition (Φ_r) for every r, then there is an explicit formula for e_n. When $s = 3$ or $p = 2$, from the results of chapter 5 and 6, we have that l_F is p - multiplicative, l_F is either 1 or 0, and D_F satisfies (Φ_r) for every r. As a consequence, in these cases we find that c is rational and $e_n - cp^{(s-1)n}$ is eventually periodic. When $s > 3$, under the condition that D_F is p - induced, we find that c is again rational, the error term Δ_n in the formula for e_n is $O(p^{(s-3)n})$ and $\Delta_{n+\lambda} = l^{\#}\Delta_n$, with fixed integers $\lambda \geq 1$ and $l^{\#}$, for large enough n. (By Monsky's appendix, D_F is always p - induced, so this holds unconditionally.) Finally we give a more explicit formula for e_n in certain cases. In particular, when $s = 3$, using a criterion for l_F to be 1 proved in chapter 5, we get a simple and precise result. We conclude with some examples, both for $s = 3$ and for $s > 3$, calculating e_n by the techniques we have developed.

1. Elementary Properties of D_F

F is a field and s is a fixed positive integer. Let $k_1, \ldots, k_s$ be non-negative integers.

Definition 1.1. *$D_F(k_1, \ldots, k_s)$ is the dimension of the vector space*

$$F[x_1, \ldots, x_s]/(x_1 + \cdots + x_s, x_1^{k_1}, \ldots, x_s^{k_s}).$$

We first show that e_n can be expressed in terms of D_F.

Lemma 1.2. *Let q, $d_1, \ldots, d_s$ be positive integers and M the vector space $F[x_1, \ldots, x_s]/(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^q, \ldots, x_s^q)$. Write $q = k_i d_i + a_i$ with $0 \leq a_i < d_i$, $1 \leq i \leq d$. Then the dimension of M over F is given by*

$$\sum_{(\epsilon_1, \ldots, \epsilon_s) \in \{0,1\}^s} \left(\prod_{\epsilon_i = 1} a_i \right) \left(\prod_{\epsilon_i = 0} (d_i - a_i) \right) D_F(k_1 + \epsilon_1, \ldots, k_s + \epsilon_s).$$

Proof. View M as a module over $F[x_1^{d_1}, \ldots, x_s^{d_s}]$. Suppose $0 \leq c_i < d_i$ and let $J \subset F[x_1^{d_1}, \ldots, x_s^{d_s}]$ be the annihilator of the cyclic submodule $M_{c_1 \cdots c_s}$ of M generated by $x_1^{c_1} \cdots x_s^{c_s}$. Let $\epsilon_i = 0$ or 1 according as $c_i \geq a_i$ or $c_i < a_i$. Then we claim that $J = \left(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^{d_1(k_1 + \epsilon_1)}, \ldots, x_s^{d_s(k_s + \epsilon_s)}\right)$.

To show this, suppose that $g \in F[x_1^{d_1}, \ldots, x_s^{d_s}]$ and that $g x_1^{c_1} \cdots x_s^{c_s} = g_0(x_1^{d_1} + \cdots + x_s^{d_s}) + g_1 x_1^q + \cdots + g_s x_s^q$. There is an obvious gradation on $F[x_1, \ldots, x_s]$ in which the degrees are elements of $\mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_s$. Since g has degree $(0, \ldots, 0)$, we may replace the g_i by appropriate homogeneous components and assume that each g_i is homogeneous in this gradation. In particular g_0 has degree $(c_1, \ldots, c_s)$ and thus can be written as $h_0 x_1^{c_1} \cdots x_s^{c_s}$ with h_0 in $F[x_1^{d_1}, \ldots, x_s^{d_s}]$. Replacing g by $g - h_0(x_1^{d_1} + \cdots + x_s^{d_s})$ we find that $g x_1^{c_1} \cdots x_s^{c_s}$ is in the ideal generated by $x_1^q, \ldots, x_s^q$. Then this is true for each monomial $x_1^{d_1 c_1'} \cdots x_s^{d_s c_s'}$ occuring in g, and we calculate that one of the $d_i c_i' + c_i$ must be $\geq q$. So one of $c_i' \geq k_i + \frac{a_i - c_i}{d_i}$; we get $J = \left(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^{d_1(k_1 + \epsilon_1)}, \ldots, x_s^{d_s(k_s + \epsilon_s)}\right)$.

This shows that the dimension of $M_{c_1 \cdots c_s}$ over F is just the dimension of $F[x_1, \ldots, x_s]/(x_1 + \cdots + x_s, x_1^{k_1 + \epsilon_1}, \ldots, x_s^{k_s + \epsilon_s})$. Since M is the direct sum of the $M_{c_1 \cdots c_s}$, the lemma follows. ∎

Now suppose p is a prime and F is the field $\mathbf{Z}/p$. Let n be a non-negative integer. Write $p^n = k_i d_i + a_i$ with $0 \le a_i < d_i, \quad 1 \le i \le s$.

Proposition 1.3. *Let e_n be the dimension of the vector space*

$$F[[x_1, \dots, x_s]]/(x_1^{d_1} + \cdots + x_s^{d_s}, x_1^{p^n}, \dots, x_s^{p^n}).$$

Then

$$e_n = \sum_{(\epsilon_1,\dots,\epsilon_s)\in\{0,1\}^s} \left(\prod_{\epsilon_i=1} a_i\right)\left(\prod_{\epsilon_i=0}(d_i - a_i)\right) D_F(k_1+\epsilon_1, \dots, k_s+\epsilon_s).$$

Proof. Since $F[[x_1,\dots,x_s]]/(x_1^{d_1}+\cdots+x_s^{d_s}, x_1^{p^n},\dots,x_s^{p^n})$ and $F[x_1,\dots,x_s]/(x_1^{d_1}+\cdots+x_s^{d_s}, x_1^{p^n},\dots,x_s^{p^n})$ have the same dimension, this follows from Lemma 1.2. ∎

Now we shall study some elementary properties of D_F.

Proposition 1.4.

(i) $D_F(k_1,\dots,k_s)$ is symmetric in the k_i.
(ii) If any of the k_i is 0, then $D_F(k_1,\dots,k_s) = 0$.
(iii) $D_F(1,\dots,1) = 1$.
(iv) $D_F(k_1,\dots,k_s,1) = D_F(k_1,\dots,k_s)$.
(v) $D_F(k_1,\dots,k_s) = \dim_F F[x_1,\dots,x_{s-1}]/(x_1^{k_1},\dots,x_{s-1}^{k_{s-1}},(x_1+\cdots+x_{s-1})^{k_s})$.
(vi) If $k_s > \sum_{i=1}^{s-1}(k_i - 1)$, then $D_F(k_1,\dots,k_s) = k_1\cdots k_{s-1}$.

Proof. (i) - (v) are obvious. If $k_s > \sum_{i=1}^{s-1}(k_i-1)$, then $(x_1+\cdots+x_{s-1})^{k_s} \in (x_1^{k_1},\dots,x_{s-1}^{k_{s-1}})$, so (vi) follows from (v). ∎

Let J be the ideal $((x_1^{k_1},\dots,x_{s-1}^{k_{s-1}}) : (x_1+\cdots+x_{s-1})^{k_s})$. Then there is an exact sequence

$$(*) \qquad 0 \longrightarrow \frac{F[x_1,\dots,x_{s-1}]}{J} \xrightarrow{(x_1+\cdots+x_{s-1})^{k_s}} \frac{F[x_1,\dots,x_{s-1}]}{(x_1^{k_1},\dots,x_{s-1}^{k_{s-1}})}$$

$$\longrightarrow \frac{F[x_1,\dots,x_{s-1}]}{(x_1^{k_1},\dots,x_{s-1}^{k_{s-1}},(x_1+\cdots+x_{s-1})^{k_s})} \longrightarrow 0.$$

Proposition 1.5.

$$D_F(k_1,\cdots,k_s) = k_1\cdots k_{s-1} - \dim_F \frac{F[x_1,\dots,x_{s-1}]}{((x_1^{k_1},\dots,x_{s-1}^{k_{s-1}}) : (x_1+\cdots+x_{s-1})^{k_s})}.$$

Proof. This follows from the exact sequence $(*)$. ∎

Now suppose F is a field of characteristic $p > 0$ and $q \geq 1$ denotes a power of p.

Proposition 1.6.

(i) If $k_1, \ldots, k_{s-1} \leq q$ and $k_s \geq q$, then $D_F(k_1, \ldots, k_s) = k_1 \cdots k_{s-1}$.

(ii) If $k_1, \ldots, k_{s-2} \leq q$ and $k_{s-1}, k_s \geq q$, then
$D_F(k_1, \ldots, k_s) = D_F(k_1, \ldots, k_{s-2}, k_{s-1} - q, k_s - q) + qk_1 \cdots k_{s-2}$.

(iii) $D_F(qk_1, \ldots, qk_s) = q^{s-1} D_F(k_1, \ldots, k_s)$.

Proof. (i) Since $k_1, \ldots, k_{s-1} \leq q$, $(x_1 + \cdots + x_{s-1})^{k_s} = (x_1^q + \cdots + x_{s-1}^q)(x_1 + \cdots + x_{s-1})^{k_s - q}$ is in $(x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}})$.
(ii) Since $k_1, \ldots, k_{s-2} \leq q$, $\left((x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}}) : (x_1 + \cdots + x_{s-1})^{k_s}\right) = \left((x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}}) : x_{s-1}^q (x_1 + \cdots + x_{s-1})^{k_s - q}\right)$, which is the same as $\left((x_1^{k_1}, \ldots, x_{s-2}^{k_{s-2}}, x_{s-1}^{k_{s-1}-q}) : (x_1 + \cdots + x_{s-1})^{k_s - q}\right)$. This means, by Proposition 1.5, that $k_1 \cdots k_{s-1} - D_F(k_1, \ldots, k_s) = k_1 \cdots k_{s-2}(k_{s-1} - q) - D_F(k_1, \ldots, k_{s-2}, k_{s-1} - q, k_s - q)$ or $D_F(k_1, \ldots, k_s) = D_F(k_1, \ldots, k_{s-2}, k_{s-1} - q, k_s - q) + qk_1 \cdots k_{s-2}$.
(iii) This follows from the fact that $F[x_1, \ldots, x_{s-1}]/(x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}}, (x_1 + \cdots + x_{s-1})^{k_s})$ is isomorphic to $F[x_1^q, \ldots, x_{s-1}^q]/(x_1^{qk_1}, \ldots, x_{s-1}^{qk_{s-1}}, (x_1 + \cdots + x_{s-1})^{qk_s})$, and $F[x_1, \ldots, x_{s-1}]/(x_1^{qk_1}, \ldots, x_{s-1}^{qk_{s-1}}, (x_1 + \cdots + x_{s-1})^{qk_s})$ is free of dimension q^{s-1} over $F[x_1^q, \ldots, x_{s-1}^q]/(x_1^{qk_1}, \ldots, x_{s-1}^{qk_{s-1}}, (x_1 + \cdots + x_{s-1})^{qk_s})$. ∎

Corollary 1.7. *Let r be a positive integer. If each $k_i \leq q$, then*

(i) $D_F(k_1, \ldots, k_{s-1}, rq + k_s) = k_1 \cdots k_{s-1}$.

(ii) $D_F(k_1, \ldots, k_{s-2}, rq + k_{s-1}, rq + k_s) = D_F(k_1, \ldots, k_s) + rqk_1 \cdots k_{s-2}$

Proof. (i) is immediate from Proposition 1.6 (i).
(ii) Using Proposition 1.6. (ii) repeatedly, we get $D_F(k_1, \ldots, k_{s-2}, rq + k_{s-1}, rq + k_s) = D_F(k_1, \ldots, k_{s-2}, (r-1)q + k_{s-1}, (r-1)q + k_s) + qk_1 \cdots k_{s-2} = \cdots = D_F(k_1, \ldots, k_s) + rqk_1 \cdots k_{s-2}$. ∎

2. Matrices of binomial coefficients and the calculation of $[k_1, k_2, k_3]_F$

We calculate $D_F(k_1, k_2, k_3)$ where k_1, k_2, k_3 are non-negative integers. When $k_3 \geq k_1 + k_2$, we already know, by Proposition 1.4 (vi), that $D_F(k_1, k_2, k_3) = k_1 k_2$. So the case of interest is when k_1, k_2, k_3 satisfy the triangle inequalities, i.e. $k_1 + k_2 \leq k_3$, $k_2 + k_3 \leq k_1$ and $k_1 + k_3 \leq k_2$, or equivalently that the largest k_i is $\leq$ the sum of the other two.

Let F be a field and $g_1, \ldots, g_s$ homogeneous elements of $F[x_1, x_2]$ generating an (x_1, x_2) - primary ideal. Let $N \subset (F[x_1, x_2])^s$ be the module of relations between the g_i. Then there is an exact sequence

$$0 \longrightarrow N \longrightarrow (F[x_1, x_2])^s \longrightarrow F[x_1, x_2] \longrightarrow F[x_1, x_2]/(g_1, \ldots, g_s) \longrightarrow 0$$

and the Hilbert syzygy theorem tells us that N is free on $s - 1$ (homogeneous) generators.

Suppose now that $s = 3$ and that (g_1, g_2) is (x_1, x_2) - primary. Let $k_i = \deg g_i$. Suppose that $g_3 \notin (g_1, g_2)$. We shall show that $\big((g_1, g_2) : g_3\big)$ is generated by two homogeneous elements whose degrees sum to $k_1 + k_2 - k_3$.

Let (u_1, u_2, u_3) and (v_1, v_2, v_3) generate N. Then u_3 and v_3 evidently generate $\big((g_1, g_2) : g_3\big)$. Since $g_3 \notin (g_1, g_2)$, u_3 and v_3 generate an (x_1, x_2) - primary ideal. Since $u_1 g_1 + u_2 g_2 + u_3 g_3 = v_1 g_1 + v_2 g_2 + v_3 g_3 = 0$, $(u_1 v_3 - v_1 u_3) g_1 + (u_2 v_3 - v_2 u_3) g_2 = 0$. Thus $\deg(u_1 v_3 - v_1 u_3) \geq \deg g_2 = k_2$, $\deg u_3 + k_3 - k_1 + \deg v_3 \geq k_2$ and $\deg u_3 + \deg v_3 \geq k_1 + k_2 - k_3$. On the other hand, $(g_2, -g_1, 0) \in N$. So $(g_2, -g_1, 0) = A(u_1, u_2, u_3) + B(v_1, v_2, v_3)$ for some homogeneous A and B. Clearly A is non-zero. Since $Au_3 + Bv_3 = 0$ and (u_3, v_3) is (x_1, x_2) - primary, $\deg A \geq \deg v_3$. Now $Au_1 + Bv_1 = g_2$. So $k_2 = \deg g_2 = \deg Au_1 \geq \deg v_3 + (\deg u_3 + k_3 - k_1)$ and $\deg u_3 + \deg v_3 \leq k_1 + k_2 - k_3$.

Now let (k_1, k_2, k_3) be a triple of non-negative integers. By the results above, the ideal $J = \big((x^{k_1}, y^{k_2}) : (x + y)^{k_3}\big)$ in $F[x, y]$ is either (1) or is generated by two homogeneous elements whose degrees sum to $k_1 + k_2 - k_3$.

Suppose that k_1, k_2 and k_3 satisfy the triangle inequalities. We shall use this result to define a non-negative element $[k_1, k_2, k_3]_F$ (often abbreviated to $[k]_F$) of $\frac{1}{2}\mathbf{Z}$.

Definition 2.1. *If $J = (1)$, $[k]_F = \frac{k_1+k_2-k_3}{2}$. If $J \neq (1)$, $[k]_F$ is chosen so $[k]_F \geq 0$ and the generators of J have degrees $\frac{k_1+k_2-k_3}{2} - [k]_F$ and $\frac{k_1+k_2-k_3}{2} + [k]_F$.*

Lemma 2.2.

$$\begin{aligned} D_F(k_1,k_2,k_3) &= k_1k_2 - \left(\frac{(k_1+k_2-k_3)^2}{4} - [k]_F^2\right) \\ &= \frac{2k_1k_2 + 2k_1k_3 + 2k_2k_3 - k_1^2 - k_2^2 - k_3^2}{4} + [k]_F^2. \end{aligned}$$

Proof. $D_F(k_1,k_2,k_3) = \dim_F F[x,y]/(x^{k_1},y^{k_2}) - \dim_F F[x,y]/J$ and J is a complete intersection. ∎

Theorem 2.3. *Set $\alpha = k_1 + k_2 - k_3$ and $\mu = \frac{\alpha-2}{2}$.*

(i) Suppose α is even. Then $[k]_F = 0$ if and only if $(x+y)^{k_3}$ is not a zero-divisor on the degree μ component of $F[x,y]/(x^{k_1},y^{k_2})$. If these conditions hold,

$$D_F(k_1,k_2,k_3) = \frac{2k_1k_2 + 2k_1k_3 + 2k_2k_3 - k_1^2 - k_2^2 - k_3^2}{4}.$$

(ii) Suppose α is odd. Then $[k]_F = \frac{1}{2}$ if and only if $(x+y)^{k_3}$ is not a zero-divisor on the degree $\mu - \frac{1}{2}$ component of $F[x,y]/(x^{k_1},y^{k_2})$. If these conditions hold,

$$D_F(k_1,k_2,k_3) = \frac{2k_1k_2 + 2k_1k_3 + 2k_2k_3 - k_1^2 - k_2^2 - k_3^2 + 1}{4}.$$

Proof. (i) $(x+y)^{k_3}$ is not a zero-divisor on this component if and only if $\left(J/(x^{k_1},y^{k_2})\right)_\mu = 0$. Since k_1 and k_2 are $> \mu$, this is the same as saying that $J_\mu = 0$, or that each generator of J has degree $\geq \mu + 1 = \frac{\alpha}{2}$. This is the same as saying that $[k]_F = 0$. Now apply Lemma 2.2.
(ii) $(x+y)^{k_3}$ is not a zero-divisor on this component if and only if $J_{\mu-\frac{1}{2}} = 0$, i.e. if and only if each generator of J has degree $\geq \mu + \frac{1}{2} = \frac{\alpha-1}{2}$. This is the same as saying that $[k]_F = \frac{1}{2}$, and Lemma 2.2 gives the final claim. ∎

We next show how to relate $[k]_F$ to the rank of a certain matrix whose entries are binomial coefficients, viewed as elements of F.

Lemma 2.4. *Set $\alpha = k_1 + k_2 - k_3$, $\mu = \frac{\alpha-2}{2}$ and let n be an integer such that $|n - \mu| \leq [k]_F$. Then the dimension of $\left(F[x,y]/J\right)_n$ is $\frac{\alpha}{2} - [k]_F$.*

Proof. Under our hypotheses on n, $n < \frac{\alpha}{2} + [k]_F$ and $n - \frac{\alpha}{2} + [k]_F \geq -1$. Now $\dim\left(F[x,y]/J\right)_n = n + 1 - \dim J_n$. Since $n < \frac{\alpha}{2} + [k]_F$, J_n consists of multiples of of a single element of degree $\frac{\alpha}{2} - [k]_F$, and $\dim J_n = \dim F[x,y]_{n-\frac{\alpha}{2}+[k]_F}$. Since $n - \frac{\alpha}{2} + [k]_F \geq -1$, this last dimension is $n + 1 - \frac{\alpha}{2} + [k]_F$, giving the lemma. ∎

Proposition 2.5. *Suppose that $k_2 \leq k_3$. Let $\alpha = k_1 + k_2 - k_3$ and M be the matrix*

$$\left(\binom{k_3}{k_3 - k_2 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha}{2}\right],\ 1 \leq j \leq \alpha - \left[\frac{\alpha}{2}\right],$$

where the binomial coefficients are viewed as elememts of F. Then $[k]_F = \frac{\alpha}{2} - \mathrm{rank}M$.

Proof. Let $R = \oplus_{j=0}^{\infty} R_j$ be the graded ring $F[x,y]/(x^{k_1}, y^{k_2})$ and $\varphi_j : R_j \to R_{j+k_3}$ be induced by multiplication by $(x+y)^{k_3}$. Set $\mu = \frac{\alpha-2}{2}$. The triangle inequalities show that $\mu + \frac{1}{2} <$ both k_1 and k_2.

Suppose α is even. Then R_μ has an F - basis $\{x^{\mu-j+1}y^{j-1}\}$, $1 \leq j \leq \mu + 1$. $R_{\mu+k_3}$ has an F - basis $\{x^{\mu+k_3-k_2+i}y^{k_2-i}\}$, $1 \leq i \leq \mu+1$. (Note that when $i = \mu+1$, $\mu + k_3 - k_2 + i = k_1 - 1$.) Furthermore M is the matrix for φ_μ with respect to the above bases. So $\mathrm{rank}M = \dim(R_\mu/\ker\varphi_\mu) = \dim(F[x,y]/J)_\mu$; Lemma 2.4 with $n = \mu$ shows this to be $\frac{\alpha}{2} - [k]_F$.

If α is odd, we make a similar argument with the map $\varphi_{\mu+\frac{1}{2}}$ using the facts: $R_{\mu+\frac{1}{2}}$ has an F - basis $\{x^{\mu-j+\frac{3}{2}}y^{j-1}\}$, $1 \leq j \leq \mu + \frac{3}{2}$ and $R_{\mu+\frac{1}{2}+k_3}$ has an F -basis $\{x^{\mu+\frac{1}{2}+k_3-k_2+i}y^{k_2-i}\}$, $1 \leq i \leq \mu + \frac{1}{2}$. ∎

Proposition 2.6.

(i) $[k_1, k_2, k_3]_F$ is symmetric in the k_i.

(ii) $[k_1 + 1, k_2, k_3]_F$ and $[k_1, k_2, k_3]_F$ differ by $\frac{1}{2}$.

(iii) If k_1', k_2', k_3' are non-negative integers satisfying the triangle inequalities, then $[k_1, k_2, k_3]_F$ and $[k_1', k_2' k_3']_F$ differ by at most $\frac{1}{2}\sum_{i=1}^{3} |k_i - k_i'|$.

Proof. (i) is immediate from Lemma 2.2. (iii) will follow from (ii).

We now prove (ii). Let M, α be associated with $[k_1, k_2, k_3]_F$ and M', α' with $[k_1 + 1, k_2, k_3]_F$.

If $k_1 < k_2 \leq k_3$, then $\alpha = k_1 + k_2 - k_3$, $\alpha' = \alpha + 1$,

$$M = \left(\binom{k_3}{k_3 - k_2 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha}{2}\right],\ 1 \leq j \leq \alpha - \left[\frac{\alpha}{2}\right]$$

and

$$M' = \left(\binom{k_3}{k_3 - k_2 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha+1}{2}\right],\ 1 \leq j \leq \alpha + 1 - \left[\frac{\alpha+1}{2}\right].$$

So M' is obtained from M by adding a row at the bottom or a column at the right according as α is odd or even. Therefore $\mathrm{rank}M' = \mathrm{rank}M$ or $\mathrm{rank}M + 1$, giving the result.

If $k_2 \leq k_1 < k_3$, then $\alpha = k_1 + k_2 - k_3$, $\alpha' = \alpha + 1$,

$$M = \left(\binom{k_3}{k_3 - k_1 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha}{2}\right], \ 1 \leq j \leq \alpha - \left[\frac{\alpha}{2}\right]$$

and

$$M' = \left(\binom{k_3}{k_3 - k_1 - 1 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha + 1}{2}\right], \ 1 \leq j \leq \alpha + 1 - \left[\frac{\alpha + 1}{2}\right].$$

So M' is obtained from M by adding a row at the top or a column at the left according as α is odd or even. Thus $\mathrm{rank}M' = \mathrm{rank}M$ or $\mathrm{rank}M + 1$, again giving the result.

If $k_2 \leq k_3 \leq k_1$, then $\alpha = k_2 + k_3 - k_1$, $\alpha' = \alpha - 1$,

$$M = \left(\binom{k_1}{k_1 - k_3 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha}{2}\right], \ 1 \leq j \leq \alpha - \left[\frac{\alpha}{2}\right]$$

and

$$M' = \left(\binom{k_1 + 1}{k_3 - k_2 + i + j - 1}\right) \qquad 1 \leq i \leq \left[\frac{\alpha - 1}{2}\right], \ 1 \leq j \leq \alpha + 1 - \left[\frac{\alpha - 1}{2}\right].$$

So M' is obtained from M by elementary row operations (adding the previous row to the next) and then removing the first row, or by elementary column operations (adding the previous column to the next) and then removing the first column according as α even or odd. Thus $\mathrm{rank}M' = \mathrm{rank}M$ or $\mathrm{rank}M - 1$, completing the proof. ∎

Proposition 2.7. *If F is a field of characteristic p, then $[pk_1, pk_2, pk_3]_F = p[k_1, k_2, k_3]_F$.*

Proof. This follows immediately from Proposition 1.6 (iii) and Lemma 2.2. ∎

When $k_1 + k_2 + k_3$ is even, the matrix associated to $[k_1, k_2, k_3]_F$ is square. Now we will determine when this matrix is non-singular, which is equivalent to when $[k_1, k_2, k_3]_F$ is zero.

Definition 2.8. *$f_{r,s}(k)$ is the determinant of the matrix*

$$\left(\binom{k}{s+i+j-1}\right) \qquad 1 \leq i \leq r, \quad 1 \leq j \leq r.$$

$f_{r,s}$ is a polynomial in k with rational coefficients.

Lemma 2.9. *The only zeros of $f_{r,s}$ are at integers in $[1-r, r+s-1]$. Moreover,*

$$(-1)^{[\frac{r}{2}]} f_{r,s}(k) = \left(\frac{k(k-1)\cdots(k-s)}{(r+s)(r+s-1)\cdots r}\right)^r \prod_{j=1}^{r-1} \left(\frac{(k-s-j)(k+j)}{(r-j)(r+s+j)}\right)^{r-j}.$$

Proof. In $\mathbf{Q}[k]$, $f_{r,s}(k)$ is divisible by $\prod_{j=0}^{r-1} \binom{k}{s+1+j}$. But the $r \times r$ matrix $\left(\binom{k}{s+i+j-1}\right)$ can be transformed by elementary column operations into the $r \times r$ matrix $\left(\binom{k+j-1}{s+i+j-1}\right)$. So $f_{r,s}$ is also divisible by $\prod_{j=1}^{r} \binom{k+j-1}{s+j}$. It follows that $f_{r,s}$ is divisible by

$$(k(k-1)\cdots(k-s))^r \prod_{j=1}^{r-1} ((k-s-j)(k+j))^{r-j}.$$

Since the degree of $f_{r,s}$ is $\leq \sum_{j=1}^{r}(s+2j-1) = sr + r^2$, $f_{r,s}$ is a constant multiple of

$$(k(k-1)\cdots(k-s))^r \prod_{j=1}^{r-1} ((k-s-j)(k+j))^{r-j}.$$

The lemma follows from the fact that $f_{r,s}(r+s) = 1$ if $r \equiv 0, 1 \pmod 4$, -1 if $r \equiv 2, 3 \pmod 4$. ∎

Remark. When char$F = 0$, Lemma 2.9 allows us to calculate $[k]_F$ and $D_F(k)$ explicitly - see Lemma 5.6.

Corollary 2.10. *If k is an integer $\geq r+s$, then*

$$(-1)^{[\frac{r}{2}]} f_{r,s}(k) = \frac{\left(\prod_{i=1}^{k+r-1} i!\right)\left(\prod_{i=1}^{k-r-s-1} i!\right)\left(\prod_{i=1}^{r+s-1} i!\right)\left(\prod_{i=1}^{r-1} i!\right)}{\left(\prod_{i=1}^{k-1} i!\right)\left(\prod_{i=1}^{k-s-1} i!\right)\left(\prod_{i=1}^{2r+s-1} i!\right)}.$$

Proof. $(k(k-1)\cdots(k-s))^r \prod_{j=1}^{r-1} ((k-s-j)(k+j))^{r-j}$ is

$$\frac{\left(\prod_{i=k}^{k+r-1} i!\right)}{\left(\prod_{i=k-r-s}^{k-s-1} i!\right)} = \frac{\left(\prod_{i=1}^{k+r-1} i!\right)\left(\prod_{i=1}^{k+r-s-1} i!\right)}{\left(\prod_{i=1}^{k-1} i!\right)\left(\prod_{i=1}^{k-s-1} i!\right)}.$$

Similarly, $\left((r+s)(r+s-1)\cdots r\right)^r \prod_{j=1}^{r-1}\left((r-j)(r+s+j)\right)^{r-j}$ is

$$\frac{\left(\prod_{i=r+s}^{2r+s-1} i!\right)}{\left(\prod_{i=1}^{r-1} i!\right)} = \frac{\left(\prod_{i=1}^{2r+s-1} i!\right)}{\left(\prod_{i=1}^{r-1} i!\right)\left(\prod_{i=1}^{r+s-1} i!\right)}.$$

Thus the corollary follows from Lemma 2.9. ∎

Definition 2.11. *Let q be a power of a prime p and k an integer $\geq r+s$. Set*

$$\alpha_q(r,s,k) = \sum_{i=1}^{k+r-1} [\frac{i}{q}] + \sum_{i=1}^{k-r-s-1} [\frac{i}{q}] + \sum_{i=1}^{r+s-1} [\frac{i}{q}] + \sum_{i=1}^{r-1} [\frac{i}{q}] - \sum_{i=1}^{k-1} [\frac{i}{q}] - \sum_{i=1}^{k-s-1} [\frac{i}{q}] - \sum_{i=1}^{2r+s-1} [\frac{i}{q}].$$

Lemma 2.12. *The exponent to which the prime p appears in $f_{r,s}(k)$ is*

$$\sum_{q=p^n,\ n\geq 1} \alpha_q(r,s,k).$$

Proof. Since the exponent to which p appears in $i!$ is $\sum_{q=p^n,\ n\geq 1} \left[\frac{i}{q}\right]$, this follows from Corollary 2.10. ∎

Let m be a positive integer and $b_{(m)}$ be the remainder when m is divided by q. Then

$$\begin{aligned}
\sum_{i=1}^{m-1} \left[\frac{i}{q}\right] &= q\left(0+1+\cdots+\left(\frac{m-b_{(m)}}{q}-1\right)\right) + b_{(m)}\left(\frac{m-b_{(m)}}{q}\right) \\
&= \frac{q}{2}\left(\frac{m-b_{(m)}}{q}-1\right)\left(\frac{m-b_{(m)}}{q}\right) + b_{(m)}\left(\frac{m-b_{(m)}}{q}\right) \\
&= \frac{1}{2q}\left(m+b_{(m)}-q\right)\left(m-b_{(m)}\right) \\
&= \frac{1}{2q}\left(m^2-qm+qb_{(m)}-b_{(m)}^2\right).
\end{aligned}$$

Since $(k+r)^2+(k-r-s)^2+(r+s)^2+r^2 = k^2+(k-s)^2+(2r+s)^2$ and $(k+r)+(k-r-s)+(r+s)+r = k+(k-s)+(2r+s)$, we find :

Lemma 2.13.

$$\begin{aligned}
\alpha_q(r,s,k) =& \frac{1}{2q}\Big(qb_{(k+r)} - b_{(k+r)}^2 + qb_{(k-r-s)} - b_{(k-r-s)}^2 + qb_{(r+s)} - b_{(r+s)}^2 \\
&+ qb_{(r)} - b_{(r)}^2 - qb_{(k)} + b_{(k)}^2 - qb_{(k-s)} + b_{(k-s)}^2 - qb_{(2r+s)} + b_{(2r+s)}^2\Big).
\end{aligned}$$

Now suppose that k_1, k_2, k_3 are non-negative integers such that $k_1 \leq k_2 \leq k_3$, $k_3 \leq k_1 + k_2$ and $k_1 + k_2 + k_3$ is even.

Corollary 2.14. *Let $2r = k_1 + k_2 - k_3$ and $s = k_3 - k_2$. Then $f_{r,s}(k_3)$ is non-zero and the exponent to which p appears in it is $\sum_{q=p^n,\ n\geq 1} \alpha_q$ where*

$$\begin{aligned}\alpha_q = \alpha_q(r,s,k_3) = &\frac{1}{2q}\Big(qb_{(\frac{k_1+k_2+k_3}{2})} - b^2_{(\frac{k_1+k_2+k_3}{2})} + qb_{(\frac{k_2+k_3-k_1}{2})} - b^2_{(\frac{k_2+k_3-k_1}{2})} \\ &+ qb_{(\frac{k_1+k_3-k_2}{2})} - b^2_{(\frac{k_1+k_3-k_2}{2})} + qb_{(\frac{k_1+k_2-k_3}{2})} - b^2_{(\frac{k_1+k_2-k_3}{2})} \\ &- qb_{(k_3)} + b^2_{(k_3)} - qb_{(k_2)} + b^2_{(k_2)} - qb_{(k_1)} + b^2_{(k_1)}\Big).\end{aligned}$$

Proof. Since $k_3 - r - s = \frac{k_2+k_3-k_1}{2} \geq 0$, the result follows from Lemmas 2.12 and 2.13 with $k = k_3$. ∎

Remark. With r and s as in Corollary 2.14, let M be the matrix

$$\left(\binom{k_3}{s+i+j-1}\right) \qquad 1 \leq i \leq r, \quad 1 \leq j \leq r$$

where the binomial coefficients are viewed as elements of F. Then $[k_1, k_2, k_3]_F = r - \operatorname{rank} M$, and $f_{r,s}(k_3)$ is the determinant of M with the binomial coefficients viewed as elements of $\mathbf{Q}$. Thus if F is a field of characteristic zero, then $[k_1, k_2, k_3]_F = 0$. Suppose now that F has characteristic $p > 0$. Then $[k_1, k_2, k_3]_F = 0$ if and only if $f_{r,s}(k_3)$ is non-zero as an element of F, which is equivalent to the condition that the exponent of p in $f_{r,s}(k_3)$ is zero, i.e. that $\sum_{q=p^n,\ n\geq 1} \alpha_q = 0$ with the α_q as in Corollary 2.14.

From now on F is a field of characteristic p. We write $[k_1, k_2, k_3]_p$ in stead of $[k_1, k_2, k_3]_F$. Now we introduce some geometry which will be used to evaluate $[k_1, k_2, k_3]_p$ explicitly.

Definition 2.15.

(i) $F \subset \mathbf{R}^3$ is the union of the planes $\sum_{i=1}^3 a_i x_i = b$, where $a_i = \pm 1$ and $b \in 2\mathbf{Z}$.

(ii) A cell is a connected component of $\mathbf{R}^3 - F$.

(iii) d^* is the metric on $\mathbf{R}^3$ defined by $d^*(P,Q) = \sum_{i=1}^3 |x_i(P) - x_i(Q)|$ for $P, Q \in \mathbf{R}^3$.

Lemma 2.16.

(i) The open unit ball B about $(1,1,1)$ in the d^* - metric is a cell, which is an open octahedron.

(ii) The cell containing $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ is an open tetrahedron T with vertices at $(0,0,0)$, $(1,1,0)$, $(1,0,1)$ and $(0,1,1)$.

Proof. (i) B is the open octahedron whose faces are the planes $x_1 + x_2 + x_3 = 2$, $x_1+x_2+x_3 = 4$, $x_1+x_2-x_3 = 0$, $x_1+x_2-x_3 = 2$, $x_1-x_2+x_3 = 0$, $x_1-x_2+x_3 = 2$, $-x_1 + x_2 + x_3 = 0$ and $-x_1 + x_2 + x_3 = 2$. Since these planes are all in F and $d^*\big((1,1,1),F\big) = 1$, B is a cell.

(ii) The planes $x_1 + x_2 - x_3 = 0$, $x_1 - x_2 + x_3 = 0$, $-x_1 + x_2 + x_3 = 0$ and $x_1 + x_2 + x_3 = 2$ bound a closed tetrahedron with vertices at $(0,0,0)$, $(1,1,0)$, $(1,0,1)$ and $(0,1,1)$. Since these planes are all in F and no point of the open tetrahedron is in F, the open tetrahedron is a cell. ∎

Lemma 2.17.

(i) F is stable under translation by $\mathbf{Z}^3_{even}$, where $\mathbf{Z}^3_{even}$ consists of all points of $\mathbf{Z}^3$ with even sum.

(ii) Every cell is a translate by $\mathbf{Z}^3_{even}$ of B, T or $-T$. (So we have a honeycomb of $\mathbf{R}^3$ by octahedra and tetrahedra. This honeycomb is known as the semi - regular honeycomb.)

(iii) If $m > n$, then $p^m F \subset p^n F$ for any integers n and m.

(iv) If C is a cell, then $\frac{1}{p^n}C$ is contained in a cell (not necessarily of the same kind) for any $n \geq 0$.

Proof. (i) is obvious.

(ii) By (i), it is enough to check this for cells containing an $(x_1, x_2, x_3) \in \mathbf{R}^3$, $0 \leq x_i \leq 1$, or an $(x_1, x_2, x_3) \in \mathbf{R}^3$, $-1 \leq x_i \leq 0$. We may assume that $0 \leq x_i \leq 1$. Then (x_1, x_2, x_3) is either in T or in the closed d^* - unit ball centered at $(1,1,1)$, $(1,0,0)$, $(0,1,0)$ or $(0,0,1)$. Since these balls are all translates of one another under $\mathbf{Z}^3_{even}$, the result follows.

(iii) follows from the fact that $p^n | p^m$.

(iv) If there is a point Q in both $\frac{1}{p^n}C$ and F, $p^n Q \in C \cap p^n F \subset C \cap F = \emptyset$, a contradiction. So $\frac{1}{p^n}C$ does not meet F ; since it is connected, it is contained in a cell. ∎

Definition 2.18. *A point $P \in \mathbf{R}^3$ is tetrahedral (resp. octahedral) if it is in a translate by $\mathbf{Z}^3_{even}$ of T or $-T$ (resp. of B).*

We shall now give a simple geometric description of the α_q of Corollary 2.14. This description shows that each $\alpha_q \geq 0$, and $\alpha_q > 0$ precisely when the point $\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_3}{q}\right)$ is octahedral.

Definition 2.19. *$g : \mathbf{R} \to \mathbf{R}$ is the function of period 1 whose restriction to $[0,1]$*

is $x - x^2$. *If* $(y_1, y_2, y_3) \in \mathbf{R}^3$, *then set*

$$\begin{aligned}\beta(y_1, y_2, y_3) =& g\left(\frac{y_1+y_2+y_3}{2}\right) + g\left(\frac{y_2+y_3-y_1}{2}\right) + g\left(\frac{y_1+y_3-y_2}{2}\right)\\ &+ g\left(\frac{y_1+y_2-y_3}{2}\right) - g(y_1) - g(y_2) - g(y_3).\end{aligned}$$

Theorem 2.20. *If* (y_1, y_2, y_3) *is octahedral,* $\beta(y_1, y_2, y_3)$ *is* $d^*\big((y_1, y_2, y_3), F\big)$. *Otherwise* $\beta(y_1, y_2, y_3) = 0$.

Proof. Since g is continuous, so is β. So it suffices to prove the result when (y_1, y_2, y_3) is tetrahedral or octahedral and no $y_i \in \mathbf{Z}$.

Let G be the group generated by translations by elements of $\mathbf{Z}^3_{even}$ together with the maps $(x_1, x_2, x_3) \mapsto (\epsilon_1 x_1, \epsilon_2 x_2, \epsilon_3 x_3)$, $\epsilon_i = \pm 1$. The elements of G are d^* - isometries taking F to F. Furthermore, since g is of period 1 and even, they also preserve β. So we are free to modify (y_1, y_2, y_3) by any element of G.

Suppose first that (y_1, y_2, y_3) is tetrahedral. We may assume that $(y_1, y_2, y_3) \in T$. Then each y_i is in $(0, 1)$ and the same holds for $\frac{y_2+y_3-y_1}{2}, \frac{y_1+y_3-y_2}{2}, \frac{y_1+y_2-y_3}{2}$ and $\frac{y_1+y_2+y_3}{2}$. Since

$$\frac{y_1+y_2+y_3}{2} + \frac{y_2+y_3-y_1}{2} + \frac{y_1+y_3-y_2}{2} + \frac{y_1+y_2-y_3}{2} = y_1 + y_2 + y_3,$$

and

$$\left(\frac{y_1+y_2+y_3}{2}\right)^2 + \left(\frac{y_2+y_3-y_1}{2}\right)^2 + \left(\frac{y_1+y_3-y_2}{2}\right)^2 + \left(\frac{y_1+y_2-y_3}{2}\right)^2 = y_1^2 + y_2^2 + y_3^2,$$

$\beta(y_1, y_2, y_3) = 0$.

Suppose next that (y_1, y_2, y_3) is octahedral. Then we may assume that (y_1, y_2, y_3) is in the open d^* - unit ball about $(1, 1, 1)$ and that each $y_i < 1$. Once again each $y_i \in (0, 1)$, and the same holds for $\frac{y_2+y_3-y_1}{2}$, $\frac{y_1+y_3-y_2}{2}$, and $\frac{y_1+y_2-y_3}{2}$. However $s = \frac{y_1+y_2+y_3}{2}$ is now in $(1, 2)$. Thus the term $s - s^2$ that appeared in calculating β when (y_1, y_2, y_3) was in T must be replaced by $(s-1) - (s-1)^2$, and $\beta(y_1, y_2, y_3) = \big((s-1) - (s-1)^2\big) - (s - s^2) = 2s - 2 = y_1 + y_2 + y_3 - 2 = d^*\big((y_1, y_2, y_3), F\big)$, giving the theorem. ∎

Theorem 2.21. *If* $\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_3}{q}\right)$ *is octahedral, the* α_q *of Corollary 2.14 is*

$$\frac{1}{2} d^*\big((k_1, k_2, k_3), qF\big).$$

Otherwise, $\alpha_q = 0$.

Proof. If k is an integer, let $b_{(k)}$ be the remainder when k is divided by q. Then

$$g\left(\frac{k}{q}\right) = g\left(\frac{b_{(k)}}{q}\right) = \frac{1}{q^2}\left(qb_{(k)} - b_{(k)}^2\right).$$

It follows that the α_q of Corollary 2.14 is just

$$\frac{q}{2}\beta\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_2}{q}\right).$$

If $\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_2}{q}\right)$ is octahedral, the preceding theorem shows this to be

$$\frac{q}{2}d^*\left(\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_2}{q}\right), F\right) = \frac{1}{2}d^*((k_1, k_2, k_3), qF).$$

If $\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_2}{q}\right)$ is not octahedral, the preceding theorem shows that $\alpha_q = 0$. ∎

Corollary 2.22. *$\alpha_q \geq 0$; equality holds precisely when $\left(\frac{k_1}{q}, \frac{k_2}{q}, \frac{k_2}{q}\right)$ is not octahedral.*

Theorem 2.23. *Let k_1, k_2, k_3 be non-negative integers satisfying the triangle inequalities. Then the following are equivalent :*

(i) No point $\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_2}{p^n}\right)$, $n \geq 0$, is octahedral.

(ii) $[k_1, k_2, k_3]_p = 0$.

Proof. If $k_1 + k_2 + k_3$ is odd, (k_1, k_2, k_3) is octahedral and $[k_1, k_2, k_3]_p$ is half an odd integer. So both (i) and (ii) are false. Suppose $k_1 + k_2 + k_3$ is even. Then Corollary 2.14 shows that $[k_1, k_2, k_3]_p = 0$ if and only if $\sum_{q=p^n,\ n\geq 1} \alpha_q = 0$. By Corollary 2.22, this happens if and only if the $\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right)$ with $n \geq 1$ are all non-octahedral. Since (k_1, k_2, k_3) is non-octahedral, the result follows. ∎

Using a little more geometry we can give an explicit description of $[k]_p$ in general.

Lemma 2.24. *Let x_1, x_2, x_3 be non-negative integers satisfying the triangle inequalities with $x_1 + x_2 + x_3$ odd. Suppose that $\left(\frac{x_1}{p^n}, \frac{x_2}{p^n}, \frac{x_3}{p^n}\right)$ is not octahedral for any $n \geq 1$.*

(i) If y_1, y_2, y_3 are non-negative integers with $\sum |y_i - p^m x_i| = p^m$ for some $m \geq 0$, then $[y_1, y_2, y_3]_p = 0$.

(ii) $[x_1, x_2, x_3]_p = \frac{1}{2}$.

Proof. It is easy to see that y_1, y_2, y_3 also satisfy the triangle inequalities. (If $x_1 \leq x_2 \leq x_3$ and $x_1 + x_2 > x_3$, then $y_1 + y_2 - y_3 \geq p^m x_1 + p^m x_2 - p^m x_3 - p^m =$

$p^m(x_1+x_2-x_3-1) \geq 0$.) Let B' be the open d^* - unit ball about (x_1, x_2, x_3). If $n \geq 1$, Lemma 2.17 shows that $p^{-n}B'$ is contained in some open cell B_n. Since $\left(\frac{x_1}{p^n}, \frac{x_2}{p^n}, \frac{x_3}{p^n}\right) \in p^{-n}B'$, B_n must be tetrahedral. Since $\sum \epsilon_i(y_i - p^m x_i) = p^m$, $(y_1, y_2, y_3) \in p^m F$. Therefore for $n \leq m$, $(y_1, y_2, y_3) \in p^n F$ and hence $\left(\frac{y_1}{p^n}, \frac{y_2}{p^n}, \frac{y_3}{p^n}\right)$ is not octahedral. Furthermore $\left(\frac{y_1}{p^n}, \frac{y_2}{p^n}, \frac{y_3}{p^n}\right) \in \overline{B'}$. It follows that for $n \geq 1$, $\left(\frac{y_1}{p^{m+n}}, \frac{y_2}{p^{m+n}}, \frac{y_3}{p^{m+n}}\right) \in \overline{B_n}$ and is not octahedral. Theorem 2.23 gives (i). In particular $[x_1+1, x_2, x_3]_p = 0$ and (ii) follows. ∎

Theorem 2.25. *Let k_1, k_2, k_3 be non-negative integers satisfying the triangle inequalities. Suppose $\left(\frac{k_1}{p^m}, \frac{k_2}{p^m}, \frac{k_3}{p^m}\right)$ is octahedral for some $m \geq 0$; choose m as large as possible. (Note that if n is large, $\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right) \in \overline{T}$, and so is not octahedral.) Then*

$$[k_1, k_2, k_3]_p = \frac{1}{2} d^*\left((k_1, k_2, k_3), p^m F\right).$$

Proof. Let (x_1, x_2, x_3) be the center of the octahedral cell, B', containing $\left(\frac{k_1}{p^m}, \frac{k_2}{p^m}, \frac{k_3}{p^m}\right)$. Then x_1, x_2, x_3 are non-negative integers satisfying the triangle inequalities with $x_1+x_2+x_3$ odd. If $n \geq 1$, $p^{-n}B'$ is contained in some open cell B_n; since this cell contains $\left(\frac{k_1}{p^{m+n}}, \frac{k_2}{p^{m+n}}, \frac{k_3}{p^{m+n}}\right)$, it is tetrahedral. So $\left(\frac{x_1}{p^n}, \frac{x_2}{p^n}, \frac{x_3}{p^n}\right)$ is not octahedral and the conclusions of Lemma 2.24 hold. Set $D = d^*\left((k_1, k_2, k_3), p^m F\right)$. Then D is the d^* - distance of (k_1, k_2, k_3) from the boundary of $p^m B'$; it follows that $D = p^m - d^*\left((k_1, k_2, k_3), (p^m x_1, p^m x_2, p^m x_3)\right)$. By Proposition 2.6,

$$\begin{aligned} [k_1, k_2, k_3]_p &\geq [p^m x_1, p^m x_2, p^m x_3]_p - \frac{1}{2} d^*\left((k_1, k_2, k_3), (p^m x_1, p^m x_2, p^m x_3)\right) \\ &= \frac{p^m}{2} - \frac{p^m - D}{2} = \frac{D}{2}. \end{aligned}$$

To obtain the opposite inequality, set $y_1 = k_1$, $y_2 = k_2$ and choose y_3 so that $\sum |y_i - p^m x_i| = p^m$ and that furthermore if $k_3 - p^m x_3$ is positive (resp. negative), so is $y_3 - p^m x_3$. This is possible since $\sum |k_i - p^m x_i| \leq p^m$; note also that $|y_3 - p^m x_3| \geq |k_3 - p^m x_3|$. By Lemma 2.24, $[y]_p = 0$. By Proposition 2.6,

$$[k]_p \leq \frac{1}{2}|y_3 - k_3| = \frac{1}{2}\left(\sum |y_i - p^m x_i| - \sum |k_i - p^m x_i|\right) = \frac{1}{2}\left(p^m - d^*(k, p^m x)\right);$$

as we saw in the last paragraph, this is $\frac{D}{2}$. ∎

There are a number of ways of restating Theorem 2.25 ; we shall offer one and use it to describe a continuous extension of $k \mapsto [k]_p$ satisfying the homogeneity condition $[pr]_p = p[r]_p$.

Definition 2.26. *Θ is the union of all the closed tetrahedral cells in the semi-regular honeycomb.*

Theorem 2.27. *Let $k = (k_1, k_2, k_3)$ where the k_i are non-negative integers satisfying the triangle inequalities. Then*

$$[k]_p = \frac{1}{2} \max_{n \in \mathbf{Z},\, n \geq 0} d^*(k, p^n \Theta).$$

Proof. If n is large, $k \in p^n \overline{T}$ and $d^*(k, p^n\Theta) = 0$; thus the maximum exists. Note that $d^*(k, p^n\Theta) > 0$ if and only if $p^{-n}k$ is octahedral, and in this case $d^*(k, p^n\Theta) = d^*(k, p^nF) = 0$. Suppose that $d^*(k, p^n\Theta)$ and $d^*(k, p^m\Theta)$ are both > 0. If $m > n$, then $p^mF \subset p^nF$, so $d^*(k, p^mF) \geq d^*(k, p^nF)$. Thus the largest value of n such that $p^{-n}k$ is octahedral provides the largest value of $d^*(k, p^n\Theta)$. If no such n exists, Theorem 2.23 shows that $[k]_p = 0$. If such an n exists and is chosen as large as possible, Theorem 2.25 shows that $[k]_p = \frac{1}{2}d^*(k, p^nF) = \frac{1}{2}d^*(k, p^n\Theta)$. ∎

Remark. Suppose $n < 0$. If $\sum k_i$ is even, then $k \in p^nF$ and $d^*(k, p^n\Theta) = 0$; while if $\sum k_i$ is odd, then $d^*(k, p^n\Theta) < 1 = d^*(k, \Theta)$. So the restriction $n \geq 0$ in the statement of Theorem 2.27 can be dropped.

Definition 2.28. *Suppose $r = (r_1, r_2, r_3)$ where the r_i are non-negative real numbers satisfying the triangle inequalities. Let $[r]_p$ be the non-negative real number*

$$\frac{1}{2} \max_{n \in \mathbf{Z}} d^*(r, p^n\Theta).$$

Remark. For n large, $d^*(r, p^n\Theta) = 0$. Also as $n \to -\infty$, $d^*(r, p^n\Theta) \to 0$. So the maximum exists.

Theorem 2.29.

(i) The restriction of $r \mapsto [r]_p$ to the points with integer coordinates is the function of Definition 2.1.

(ii) $r \mapsto [r]_p$ is continuous ; in fact $|[r]_p - [r']_p| \leq \frac{1}{2}d^*(r, r')$.

(iii) $[pr]_p = p[r]_p$.

(iv) If the coordinates of r are rational, $[r]_p$ is rational.

Proof. (i) is immediate from the remark following Theorem 2.27. (ii) and (iv) follow directly from the definition of $[r]_p$. Finally since $d^*(pr, pr') = pd^*(r, r')$, $d^*(pr, p^n\Theta) = pd^*(r, p^{n-1}\Theta)$, giving (iii). ∎

Let d_1, d_2, d_3 be positive integers and e_n be the F dimension of

$$F[[x_1, x_2, x_3]]/(x_1^{d_1} + x_2^{d_2} + x_3^{d_3}, x_1^{p^n}, x_2^{p^n}, x_3^{p^n}).$$

We know from [1] that $e_n = cp^{2n} + O(p^n)$ for some positive real c. We now identify c explicitly and show that it is rational. In chapter 7 we shall see that $e_n = cp^{2n} +$ (an eventually periodic function of n).

Theorem 2.30. *Let e_n be defined as above. Then*

$$\lim_{n\to\infty} p^{-2n} e_n = c$$

where

(i) $c = \frac{d_1+d_2+d_3}{2} - \frac{d_1d_2}{4d_3} - \frac{d_1d_3}{4d_2} - \frac{d_2d_3}{4d_1} + d_1d_2d_3\left[\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right]_p^2$ *if* $\left(\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right)$ *satisfies the triangle inequalities.*

(ii) $c = \min(d_1, d_2, d_3)$ *otherwise.*

Proof. We may assume that $d_1 \le d_2 \le d_3$. Set

$$H(r_1, r_2, r_3) = \frac{r_1r_2 + r_1r_3 + r_2r_3}{2} - \frac{r_1^2 + r_2^2 + r_3^2}{4} = r_2r_3 - \left(\frac{r_1 - r_2 - r_3}{2}\right)^2.$$

Extend the function $[r_1, r_2, r_3]_p$ of Definition 2.28 to all of $[0, \infty)^3$ by setting

$$[r_1, r_2, r_3]_p = \frac{r_1 - r_2 - r_3}{2}$$

if $r_1 \ge r_2 + r_3$, and making similar definitions if $r_2 \ge r_1 + r_3$ or $r_3 \ge r_1 + r_2$. The new function we get still satisfies (ii), (iii) and (iv) of Theorem 2.29. Furthermore if k_1, k_2, k_3 are any non-negative integers,

$$D_F(k_1, k_2, k_3) = H(k_1, k_2, k_3) + [k_1, k_2, k_3]_p^2.$$

By Lemma 1.2, e_n is the sum of $d_1d_2d_3$ terms, each of the form $H(k_1, k_2, k_3) + [k_1, k_2, k_3]_p^2$ with $\left|k_i - \frac{p^n}{d_i}\right| \le 1$. So $p^{-2n}e_n$ is a sum of $d_1d_2d_3$ terms, each of the form

$$H\left(\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right) + \left[\frac{k_1}{p^n}, \frac{k_2}{p^n}, \frac{k_3}{p^n}\right]_p^2.$$

Letting $n \to \infty$ we find that

$$p^{-2n}e_n \to d_1d_2d_3\left(H\left(\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right) + \left[\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right]_p^2\right).$$

If $\frac{1}{d_1} \le \frac{1}{d_2} + \frac{1}{d_3}$, $\left(\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right)$ satisfies the triangle inequalities and we get (i). If $\frac{1}{d_1} \ge \frac{1}{d_2} + \frac{1}{d_3}$, $H\left(\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right) + \left[\frac{1}{d_1}, \frac{1}{d_2}, \frac{1}{d_3}\right]_p^2$ is easily seen to be $\frac{1}{d_2d_3}$, so we get (ii). ∎

3. Matrices of multinomial coefficients and a functional equation for D_F

p is a prime and F is a field of characteristic p. $q \geq 1$ denotes a power of p. $k_1, \ldots, k_{s-2}$ and μ_2 are non-negative integers and α is an integer. Set $r = (k_1 - 1, \ldots, k_{s-2} - 1)$.

Let $\mu_1 = \alpha - s + 1 - \mu_2$,
$S_1 = \left\{a = (a_1, \ldots, a_{s-2}) \in \mathbf{Z}^{s-2} \;\mid\; a_i \geq 0, \;\; a_1 + \cdots + a_{s-2} \leq \mu_1\right\}$,
$S_2 = \left\{b = (b_1, \ldots, b_{s-2}) \in \mathbf{Z}^{s-2} \;\mid\; b_i \geq 0, \;\; b_1 + \cdots + b_{s-2} \leq \mu_2\right\}$.

Definition 3.1.

(i) *If $k \in \mathbf{Z}$ and $N \in \mathbf{Z}^{s-2}$ with each $N_i \geq 0$, set*

$$\left(\frac{k}{N}\right) = \frac{(\sum N_i)!}{\prod(N_i!)}\binom{k}{\sum N_i}.$$

If any $N_i < 0$, set

$$\left(\frac{k}{N}\right) = 0.$$

(ii) *$M(k)$ is the matrix with rows indexed by S_1 and columns indexed by S_2, whose entry in place (a, b), $a \in S_1$, $b \in S_2$, is*

$$\left(\frac{k}{r - a - b}\right).$$

Remark. If $k \geq 0$, $\left(\frac{k}{N}\right)$ is just the coefficient of $\left(\prod_1^{s-2} x_i{}^{N_i}\right) x_{s-1}^{k - \Sigma N_i}$ in $\left(\sum_1^{s-1} x_i\right)^k$.

Lemma 3.2. *Suppose each k_i $(1 \leq i \leq s-2)$ is $\leq q$ and that $k \in \mathbf{Z}$. Then the matrices $M(k)$ and $M(q+k)$ are congruent mod p.*

Proof. The entries of $M(k)$ are rational polynomials in k and therefore continuous in the p - adic topology. So we may replace k by $k + p^l$ with l large and assume that $k \geq 0$.

Now a typical coefficient of $M(k)$ is of the form $\left(\frac{k}{N}\right)$ where each $N_i \leq r_i < q$. If $N_i < 0$, $\left(\frac{k}{N}\right) = 0 = \left(\frac{q+k}{N}\right)$. Suppose each $N_i \geq 0$. Then $\left(\frac{q+k}{N}\right)$ is the coefficient of $\left(\prod_1^{s-2} x_i{}^{N_i}\right) x_{s-1}^{q+k-\Sigma N_i}$ in $(x_1 + \cdots + x_{s-1})^{q+k}$. Now mod p, this is the coefficient of $\left(\prod_1^{s-2} x_i{}^{N_i}\right) x_{s-1}^{k-\Sigma N_i}$ in $(x_1+\cdots+x_{s-1})^{q+k}$. Now mod p, this is the coefficient of $\left(\prod_1^{s-2} x_i{}^{N_i}\right) x_{s-1}^{q+k-\Sigma N_i}$ in $(x_1+\cdots+x_{s-1})^k(x_1^q+\cdots+x_{s-1}^q)$. Since each $N_i < q$, this is the same as the coefficient of $\left(\prod_1^{s-2} x_i{}^{N_i}\right) x_{s-1}^{k-\Sigma N_i}$ in $(x_1+\cdots+x_{s-1})^k$ and this coefficient is precisely $\binom{k}{N}$. ∎

Lemma 3.3. *Suppose that $k, k' \in \mathbf{Z}$ with $k + k' = \left(\sum_1^{s-2} k_i\right) - \alpha$. Then the matrices $M(k)$ and $M(k')$ can be transformed into one another by elementary row and column transformations over* **Z**.

Proof. We first illustrate the proof in the case $s = 4$, $k_1 = k_2 = 3$, $\alpha = 6$, $\mu_2 = 2$. Then $\mu_1 + \mu_2 = 3$. So $\mu_1 = 1$, S_1 consists of the pairs $(0,0)$, $(0,1)$ and $(1,0)$, S_2 of the pairs $(0,0)$, $(0,1)$, $(1,0)$, $(0,2)$, $(1,1)$ and $(2,0)$, and $M(k)$ is the following matrix :

$$\begin{array}{c|cccccc}
 & (0,0) & (0,1) & (1,0) & (0,2) & (1,1) & (2,0) \\
\hline
(0,0) & 6\binom{k}{4} & 3\binom{k}{3} & 3\binom{k}{3} & \binom{k}{2} & 2\binom{k}{2} & \binom{k}{2} \\
(0,1) & 3\binom{k}{3} & \binom{k}{2} & 2\binom{k}{2} & 0 & \binom{k}{1} & \binom{k}{1} \\
(1,0) & 3\binom{k}{3} & 2\binom{k}{2} & \binom{k}{2} & \binom{k}{1} & \binom{k}{1} & 0
\end{array}$$

We first replace column $(0,0)$ by the sum of columns $(0,0)$, $(1,0)$ and $(0,1)$. We then replace each column (b_1, b_2) with $b_1 + b_2 = 1$ by the sum of columns (b_1, b_2), (b_1+1, b_2) and (b_1, b_2+1). At this point we have the matrix in which the k's in each column with $b_1 + b_2 < 2$ are replaced by $k+1$'s. If we then once again replace column $(0,0)$ by the sum of columns $(0,0)$, $(1,0)$ and $(0,1)$, we get the matrix $\left(\binom{k+2-b_1-b_2}{r-a-b}\right)$ shown below :

$$\begin{array}{c|cccccc}
 & (0,0) & (0,1) & (1,0) & (0,2) & (1,1) & (2,0) \\
\hline
(0,0) & 6\binom{k+2}{4} & 3\binom{k+1}{3} & 3\binom{k+1}{3} & \binom{k}{2} & 2\binom{k}{2} & \binom{k}{2} \\
(0,1) & 3\binom{k+2}{3} & \binom{k+1}{2} & 2\binom{k+1}{2} & 0 & \binom{k}{1} & \binom{k}{1} \\
(1,0) & 3\binom{k+2}{3} & 2\binom{k+1}{2} & \binom{k+1}{2} & \binom{k}{1} & \binom{k}{1} & 0
\end{array}$$

We now turn to row operations. Replacing row $(0,0)$ by the sum of rows $(0,0)$, $(1,0)$ and $(0,1)$, we get the matrix $\left(\binom{k+3-a_1-a_2-b_1-b_2}{r-a-b}\right)$ whose entry in position (a,b) is a certain multiple of $\binom{k+N-1}{N}$ where $N = 4 - a_1 - a_2 - b_1 - b_2$. Now $\binom{k+N-1}{N} = (-1)^N\binom{-k}{N}$. It follows that

$$\left(\binom{k+3-a_1-a_2-b_1-b_2}{r-a-b}\right) = \left((-1)^{a_1+a_2}(-1)^{b_1+b_2}\binom{-k}{r-a-b}\right).$$

So if we multiply each row (a_1, a_2) by $(-1)^{a_1+a_2}$ and each column (b_1, b_2) by $(-1)^{b_1+b_2}$, we get the matrix $M(-k)$. Now $k + k' = k_1 + k_2 - \alpha = 0$, so $k' = -k$, and $M(k)$ and $M(k')$ are indeed equivalent over $\mathbf{Z}$.

Now consider the general case. Let e_i be the vector which is 1 in the i^{th} place and 0 elsewhere. First make a series of elementary column operations on M as above, replacing some column a by the sum of columns $a + e_i$ at each step. In this way we transform $M(k)$ into $\left(\binom{k+\mu_2-\Sigma b_i}{r-a-b}\right)$. Then performing an analogous series of elementary row operations, we get

$$\left(\binom{k+\mu_1+\mu_2-\sum a_i-\sum b_i}{r-a-b}\right) = \left(\binom{k+\alpha-s+1-\sum a_i-\sum b_i}{r-a-b}\right).$$

Let $N = \sum(r_i - a_i - b_i) = \left(\sum_1^{s-2} k_i\right) - s + 2 - \sum a_i - \sum b_i$. Then the entry in position (a, b) of this last matrix is a certain multiple of $\binom{k+\alpha+N-\Sigma k_i-1}{N} = (-1)^N \binom{k'}{N}$, since $k + \alpha + N - \sum k_i - 1$ and k' add up to $N - 1$. So up to sign our matrix is

$$\left((-1)^{a_1+a_2}(-1)^{b_1+b_2}\binom{k'}{r-a-b}\right).$$

Finally, multiplying various rows and columns of this matrix by -1, we get the matrix $M(k')$. ∎

Suppose now that k_{s-1} and k_s are non-negative integers with $k_s - k_{s-1} = \left(\sum_1^{s-2} k_i\right) - \alpha$.

Definition 3.4. *$R = \oplus R_j$ is the graded ring $F[x_1, \ldots, x_{s-1}]/(x_1^{k_1}, \ldots, x_{s-1}^{k_{s-1}})$. $\varphi_{\mu_2} : R_{\mu_2} \to R_{\mu_2+k_s}$ is the map induced by multiplication by $(x_1 + \cdots + x_{s-1})^{k_s}$.*

We shall describe monomial bases for R_{μ_2} and $R_{\mu_2+k_s}$ and relate the matrix of φ_{μ_2} with respect to these bases to the matrix $M(k_s)$ of Definition 3.1.

Note first that a basis of R_{μ_2} is given by the monomials $\left(\prod_1^{s-2} x_i^{b_i}\right) x_{s-1}^{\mu_2-\Sigma b_i}$ with $0 \le b_i \le r_i$ and $0 \le \mu_2 - \sum b_i \le k_{s-1} - 1$. This last condition may be rewritten as $\sum b_i \le \mu_2$ and $\sum b_i \ge \mu_2 - k_{s-1} + 1$. So if we let

$$T_2 = \left\{ b \in S_2 \;\middle|\; b_i \le r_i, \;\; \sum b_i \ge \mu_2 - k_{s-1} + 1 \right\},$$

then the monomials $\left(\prod_1^{s-2} x_i^{b_i}\right) x_{s-1}^{\mu_2-\Sigma b_i}$, $\;b \in T_2$, form a basis of R_{μ_2}.

Note next that a basis of $R_{\mu_2+k_s}$ is given by the monomials $\left(\prod_1^{s-2} x_i^{r_i-a_i}\right) x_{s-1}^{\mu_2+k_s-\Sigma(r_i-a_i)}$ with $0 \le a_i \le r_i$ and $0 \le \mu_2 + k_s - \sum(r_i - a_i) \le$

$k_{s-1}-1$. We may rewrite this last condition as $\sum a_i \le (\sum r_i)+k_{s-1}-k_s-1-\mu_2$ and $\sum a_i \ge (\sum r_i)-k_s-\mu_2$. Now $\sum r_i = \left(\sum_1^{s-2} k_i\right) - s + 2 = k_s - k_{s-1} + \alpha - s + 2 = k_s - k_{s-1} + \mu_1 + \mu_2 + 1$. So the conditions on the a_i are that $0 \le a_i \le r_i$, that $\sum a_i \le \mu_1$ and that $\sum a_i \ge \mu_1 - k_{s-1} + 1$. If we let

$$T_1 = \left\{a \in S_1 \;\mid\; a_i \le r_i,\;\; \sum a_i \ge \mu_1 - k_{s-1} + 1\right\}$$

and observe that $(\mu_2 + k_s) - \sum(r_i - a_i) = k_{s-1} - 1 - \mu_1 + \sum a_i$, we conclude that the monomials $\left(\prod_1^{s-2} x_i^{r_i-a_i}\right) x_{s-1}^{k_{s-1}-1-\mu_1+\Sigma a_i}$, $\quad a \in T_1$, form a basis of $R_{\mu_2+k_s}$.

The matrix of φ_{μ_2} with respect to the above monomial bases is a matrix whose columns are indexed by the subset T_2 of S_2 and whose rows are indexed by the subset T_1 of S_1.

Lemma 3.5. *Let $M_1(k_s)$ be the matrix of multinomial coefficients*

$$\left(\binom{k_s}{r-a-b}\right) \qquad a \in T_1, \quad b \in T_2.$$

Then the matrix of φ_{μ_2} is the reduction modulo p of $M_1(k_s)$.

Proof. If $a \in T_1$ and $b \in T_2$, the entry (a, b) of the matrix of φ_{μ_2} is the coefficient of $\left(\prod_1^{s-2} x_i^{r_i-a_i}\right) x_{s-1}^{k_{s-1}-1-\mu_1+\Sigma a_i}$ in $(x_1+\cdots+x_{s-1})^{k_s} \left(\prod_1^{s-2} x_i^{b_i}\right) x_{s-1}^{\mu_2-\Sigma b_i}$. This is the same as the coefficient of $\left(\prod_1^{s-2} x_i^{r_i-a_i-b_i}\right) x_{s-1}^{k_s-1-\Sigma(r_i-a_i-b_i)}$ in $(x_1+\cdots+x_{s-1})^{k_s}$. By the remark after Definition 3.1 this is just $\binom{k_s}{r-a-b}$ viewed as element of F. Since F is of characteristic p the result follows. ∎

Lemma 3.6. *The matrix $M_1(k_s)$ is obtained from the matrix $M(k_s)$ by dropping certain rows and columns consisting entirely of zeros.*

Proof. Suppose $b \in S_2$ but is not in T_2. Then either $b_j > r_j$ for some j or $\sum b_i \le \mu_2 - k_{s-1}$. In the first case, $r_j - a_j - b_j < 0$ for each a in S_1, so $\binom{k_s}{r-a-b} = 0$ for each a, and column b of $M(k_s)$ is all zeros. In the second case for each $a \in S_1$, $\sum(r_i - a_i - b_i) = k_s - k_{s-1} + \mu_1 + \mu_2 + 1 - \sum a_i - \sum b_i \ge k_s - k_{s-1} + \mu_1 + \mu_2 + 1 - \mu_1 - (\mu_2 - k_{s-1}) = k_s + 1$. So $\binom{k_s}{r-a-b} = 0$ for each a and again column b of $M(k_s)$ is all zeros.

A similar argument shows that when $a \in S_1$ but is not in T_1 then row a of $M(k_s)$ is all zeros. ∎

Theorem 3.7. *Let q be a power of p and $k_1, \ldots, k_s$ integers with $0 \le k_i \le q$. Set $k'_{s-1} = q - k_s$ and $k'_s = q - k_{s-1}$ so that $k'_s - k'_{s-1} = k_s - k_{s-1}$. Let I and*

$I' \subset F[x_1, \dots, x_{s-1}]$ be the ideals $\left((x_1^{k_1}, \dots, x_{s-1}^{k_{s-1}}) : (\sum x_i)^{k_s}\right)$ and $\left((x_1^{k_1}, \dots, x_{s-1}^{k'_{s-1}}) : (\sum x_i)^{k'_s}\right)$ respectively. Then the graded rings $F[x_1, \dots, x_{s-1}]/I$ and $F[x_1, \dots, x_{s-1}]/I'$ have the same dimension ; in fact they have the same dimension in each degree.

Proof. Let μ_2 be an integer ≥ 0. We shall show that our two rings have the same dimension in degree μ_2.

Choose α so that $k'_s - k'_{s-1} = k_s - k_{s-1} = \left(\sum_1^{s-2} k_i\right) - \alpha$. Then we are in the situation described at the beginning of this chapter. Let R and R' be the graded rings $F[x_1, \dots, x_{s-1}]/(x_1^{k_1}, \dots, x_{s-1}^{k_{s-1}})$ and $F[x_1, \dots, x_{s-1}]/(x_1^{k_1}, \dots, x_{s-1}^{k'_{s-1}})$ respectively. We have maps $\varphi_{\mu_2} : R_{\mu_2} \to R_{\mu_2 + k_s}$ and $\varphi'_{\mu_2} : R'_{\mu_2} \to R'_{\mu_2 + k_s}$ induced by multiplication by $(\sum x_i)^{k_s}$ and $(\sum x_i)^{k'_s}$. φ_{μ_2} induces an isomorphism between $\left(F[x_1, \dots, x_{s-1}]/I\right)_{\mu_2}$ and $\varphi_{\mu_2}(R_{\mu_2})$. Thus the dimension of $\left(F[x_1, \dots, x_{s-1}]/I\right)_{\mu_2}$ is the rank of the matrix representing φ_{μ_2} ; by Lemmas 3.5 and 3.6 it is the rank of the reduction modulo p of $M(k_s)$. Similarly the dimension of $\left(F[x_1, \dots, x_{s-1}]/I'\right)_{\mu_2}$ is the rank of the reduction molulo p of $M(k'_s)$. Now $k'_s = q - k_{s-1}$, so in view of Lemma 3.2 it suffices to show that the modulo p reductions of $M(k_s)$ and $M(-k_{s-1})$ have the same rank. But this follows from Lemma 3.3 with $k = k_s$ and $k' = -k_{s-1}$.

∎

Theorem 3.8. *Let $k_1, \dots, k_s$ and q be as in Theorem 3.7. Then*

$$D_F(k_1, \dots, k_s) = D_F(k_1, \dots, k_{s-2}, q - k_{s-1}, q - k_s) + (k_{s-1} + k_s - q) \prod_1^{s-2} k_i.$$

Proof. Combining Theorem 3.7 with Proposition 1.5 we find that $k_{s-1} \prod_1^{s-2} k_i - D_F(k_1, \dots, k_s) = (q - k_s) \prod_1^{s-2} k_i - D_F(k_1, \dots, k_{s-2}, q - k_{s-1}, q - k_s)$, giving the theorem. ∎

4. Definition and properties of l_F

Let $t_1, \ldots, t_s$ be indeterminates over $\mathbf{Z}$. If $\epsilon = (\epsilon_1, \ldots, \epsilon_s) \in \{0,1\}^s$, let $t_\epsilon = \prod_{\epsilon_i=1} t_i$.

Definition 4.1.

(i) $M \subset \mathbf{Z}[t_1, \ldots, t_s]$ is the abelian group of rank 2^s spanned by the t_ϵ.

(ii) $M_0 \subset M$ is the rank $2^s - 1$ group spanned by the t_ϵ with $\epsilon \neq (1, \ldots, 1)$.

Remark 1. Each $f \in M$ gives a function $\{0,1\}^s \to \mathbf{Z}$ by evaluation. Note that $\prod_{\epsilon_i=1} t_i \prod_{\epsilon_i=0}(1-t_i)$ lies in M and gives a function which is 1 at a single point ϵ of $\{0,1\}^s$ and 0 elsewhere. It follows that the map from M to the additive group of functions $\{0,1\}^s \to \mathbf{Z}$ is bijective.

Remark 2. Let f be a function $\{0,1\}^s \to \mathbf{Z}$. Then when f is expressed as a $\mathbf{Z}$ - linear combination of the t_ϵ, the coefficient of $\prod_{i=1}^s t_i$ in f is $(-1)^s \sum_\epsilon (-1)^{\epsilon_1+\cdots+\epsilon_s} f(\epsilon)$.

Note that it suffices to prove this when f is represented by a monomial t_ϵ. Suppose that t_ϵ is not divisible by some t_i, for example t_1. Then $f(1, \epsilon_2, \ldots, \epsilon_s) = f(0, \epsilon_2, \ldots, \epsilon_s)$ and $\sum_\epsilon (-1)^{\epsilon_1+\cdots+\epsilon_s} f(\epsilon_1, \ldots, \epsilon_s) = 0$. If on the other hand $t_\epsilon = t_1 \cdots t_s$, then $(-1)^s \sum_\epsilon (-1)^{\epsilon_1+\cdots+\epsilon_s} \epsilon_1 \cdots \epsilon_s = (-1)^s \prod_{i=1}^s \left(\sum_0^1 (-1)^{\epsilon_i} \epsilon_i\right) = 1$.

We denote the set of non-negative integers by I_∞. An element $r = (r_1, \ldots, r_s)$ of I_∞^s is "even" if $\sum r_i$ is even, "odd" if $\sum r_i$ is odd. $\sigma(r) = (-1)^{\Sigma r_i}$. (We diverge from the notation of the previous chapters in which $\sigma(r) = \sum r_i$, but no confusion should arise.)

We shall define an integer $l_F(r)$ and an element $\varphi_{F,r}$ of M_0.

Definition 4.2. *If r is even, then $l_F(r) \in \mathbf{Z}$ and $\varphi_{F,r} \in M_0$ are chosen so that $D_F(r+\epsilon) = l_F(r)\epsilon_1 \cdots \epsilon_s + \varphi_{F,r}(\epsilon)$ for all $\epsilon \in \{0,1\}^s$.*

If on the other hand r is odd, then $l_F(r) \in \mathbf{Z}$ and $\varphi_{F,r} \in M_0$ are chosen so that $D_F(r+\epsilon) = l_F(r)(1-\epsilon_1)\epsilon_2 \cdots \epsilon_s + \varphi_{F,r}(\epsilon)$ for all $\epsilon \in \{0,1\}^s$.

Remark . If r is even, $\varphi_{F,r}$ is completely determined by the values $\varphi_{F,r}(\epsilon) = D_F(r+\epsilon)$ for $\epsilon \neq (1, \ldots, 1)$, and $l_F(r) = D_F(r_1+1, \ldots, r_s+1) - \varphi_{F,r}(1, \ldots, 1)$.

If r is odd, $\varphi_{F,r}$ is completely determined by the values $\varphi_{F,r}(\epsilon) = D_F(r+\epsilon)$ for $\epsilon \neq (0, 1, \ldots, 1)$, and $l_F(r) = D_F(r_1, r_2+1, \ldots, r_s+1) - \varphi_{F,r}(0, 1, \ldots, 1)$.

$l_F(r)$ can be written as a linear combination of the $D_F(r+\epsilon)$.

Proposition 4.3.

$$l_F(r) = (-1)^{s+\Sigma r_i} \sum_{\epsilon\in\{0,1\}^s} (-1)^{\Sigma\epsilon_i} D_F(r+\epsilon).$$

Proof. Since $l_F(r)$ is the coefficient of $t_1\cdots t_s$ in the function $f : \{0,1\}^s \to \mathbf{Z}$ defined by $f(\epsilon) = (-1)^{\Sigma r_i} D_F(r+\epsilon)$, this follows from Remark 2. ▮

Proposition 4.4.

(i) $l_F(r)$ *is symmetric in the* r_i.

(ii) $l_F(0) = 1$.

Proof. (i) is obvious. Since $D_F(\epsilon_1,\ldots,\epsilon_s) = \epsilon_1\cdots\epsilon_s$, we get (ii). ▮

Proposition 4.5.

$$D_F(r) = \sum_{0\le k\le(r_1-1,\ldots,r_s-1)} (-1)^{\Sigma k_i} l_F(k).$$

Proof. Consider the multiple sum

$$\sum_{0\le k\le(r_1-1,\ldots,r_s-1)} \sum_{\epsilon}(-1)^{\epsilon_1+\cdots+\epsilon_s} D_F(k+\epsilon).$$

Suppose $(1,\ldots,1)\le x=(x_1,\ldots,x_s)\le r$. Let us calculate the coefficient of $D_F(x)$ in the multiple sum. k makes a contribution precisely when $0\le k\le(r_1-1,\ldots,r_s-1)$ and $k=x-\epsilon$ for some ϵ ; furthermore the contribution in this case is $(-1)^{\epsilon_1+\cdots+\epsilon_s}$. Thus the coefficient of $D_F(x)$ is $\sum_{x-\epsilon\le(r_1-1,\ldots,r_s-1)}(-1)^{\epsilon_1+\cdots+\epsilon_s}$. Suppose $x\ne r$, for example $x_1<r_1$. Then $x-(0,\epsilon_2,\ldots,\epsilon_s)\le(r_1-1,\ldots,r_s-1)$ if and only if $x-(1,\epsilon_2,\ldots,\epsilon_s)\le(r_1-1,\ldots,r_s-1)$. Thus the terms in the above sum cancel in pairs and the coefficient of $D_F(x)$ is zero. If on the other hand $x=r$, the only term in the above sum is $(-1)^s$, coming from $\epsilon=(1,\ldots,1)$. So the multiple sum is $(-1)^s D_F(r)$; the proposition follows immediately from Proposition 4.3. ▮

Fix a prime p. $q\ge 1$ will always denote a power of p. We denote the set of integers in $[0,q-1]$ by I_q. Let F be a field of characteristic p.

Proposition 4.6.

(i) If $r=(r_1,\ldots,r_s)\in I_q^s$, *then*

$$l_F(r_1,\ldots,r_{s-2},q-1-r_{s-1},q-1-r_s) = l_F(r_1,\ldots,r_s).$$

(ii) For fixed $r_1, \dots, r_{s-1} \in I_q$,

$$\sum_{0 \le r_s \le q-1} (-1)^{\Sigma r_i} l_F(r_1, \dots, r_{s-1}, r_s) = 1.$$

Proof. (i) By Theorem 3.8, $D_F(k_1, \dots, k_{s-2}, k_{s-1}, q - k_s) - D_F(k_1, \dots, k_{s-2}, q - k_{s-1}, k_s) = \left(\prod_1^{s-2} k_i\right)(k_{s-1} - k_s)$. So $D_F(k_1 + \epsilon_1, \dots, k_{s-2} + \epsilon_{s-2}, k_{s-1} + \epsilon_{s-1}, q - k_s - \epsilon_s) - D_F(k_1 + \epsilon_1, \dots, k_{s-2} + \epsilon_{s-2}, q - k_{s-1} - \epsilon_{s-1}, k_s + \epsilon_s) = \left(\prod_1^{s-2}(k_i + \epsilon_i)\right)(k_{s-1} - k_s + \epsilon_{s-1} - \epsilon_s)$. On the left hand side replace $q - k_s - \epsilon_s$ by $(q - 1 - k_s) + (1 - \epsilon_s)$ and replace $q - k_{s-1} - \epsilon_{s-1}$ by $(q - 1 - k_{s-1}) + (1 - \epsilon_{s-1})$. Then multiply both sides by $(-1)^{\epsilon_1 + \cdots + \epsilon_{s-1}}$ and sum over $\epsilon_1, \dots, \epsilon_s$. The left hand side then gives $(-1)^{s+q+1+\Sigma k_i}\left(l_F(k_1, \dots, k_{s-2}, k_{s-1}, q - 1 - k_s) - l_F(k_1, \dots, k_{s-2}, q - 1 - k_{s-1}, k_s)\right)$. Since $\left(\prod_1^{s-2}(k_i + \epsilon_i)\right)(k_{s-1} - k_s + \epsilon_{s-1} - \epsilon_s)$ is a linear combination of monomials in $\epsilon_1, \dots, \epsilon_s$ with no $\epsilon_1 \cdots \epsilon_s$ term, the sum on the right hand side is zero.

(ii) When $q = 1$, this is obvious since $l_F(0) = 1$. Suppose $q > 1$. It is easy to see that $\sum_{0 \le r_s \le q-1} (-1)^{\Sigma r_i} l_F(r_1, \dots, r_s) = (-1)^{s-1} \sum_{\epsilon_1, \dots, \epsilon_{s-1} \in \{0,1\}} (-1)^{\Sigma \epsilon_i} D_F(r_1 + \epsilon_1, \dots, r_{s-1} + \epsilon_{s-1}, q)$. Since each $r_i + \epsilon_i \le q$, $D_F(r_1 + \epsilon_1, \dots, r_{s-1} + \epsilon_{s-1}, q) = \prod_{1 \le i \le s-1}(r_i + \epsilon_i)$. So

$$\begin{aligned}
\sum_{0 \le r_s \le q-1} (-1)^{\Sigma r_i} l_F(r_1, \dots, r_s) =& (-1)^{s-1} \sum_{\epsilon_1, \dots, \epsilon_{s-1} \in \{0,1\}} (-1)^{\Sigma \epsilon_i} \prod_{1 \le i \le s-1} (r_i + \epsilon_i) \\
=& (-1)^{s-1} \prod_{1 \le i \le s-1} \left((r_i + 0) - (r_i + 1)\right) \\
=& 1.
\end{aligned}$$

■

Let $e_i = (0, \dots, 0, \overset{i}{1}, 0, \dots, 0) \in I_\infty^s$.

Definition 4.7. *Let i and j be distinct elements of $\{1, \dots, s\}$. Then*

$$D_{i,j}(k) = D_F(k) - D_F(k + e_i) - D_F(k + e_j) + D_F(k + e_i + e_j).$$

Lemma 4.8. $0 \le D_{1,2}(k) \le k_4 \cdots k_s$.

Proof. Let $f = x_2 + \cdots + x_s$, $R = F[x_2, \dots, x_s]/(x_2^{k_2}, \dots, x_s^{k_s})$ and $R' = F[x_2, \dots, x_s]/(x_2^{k_2+1}, x_3^{k_3}, \dots, x_s^{k_s})$. Then the quotient map $R' \to R$ induces an onto map $f^{k_1}R'/f^{k_1+1}R' \to f^{k_1}R/f^{k_1+1}R$. Therefore $\dim_F(f^{k_1}R'/f^{k_1+1}R') \ge \dim_F(f^{k_1}R/f^{k_1+1}R)$, which gives $D_F(k + e_1 + e_2) - D_F(k + e_2) \ge D_F(k + e_1) - D_F(k)$, i.e. $D_{1,2}(k) \ge 0$.

To show the second inequality, choose q a power of p such that $k_1, k_2 \leq q-1$ and $k_3, \ldots, k_s \leq q$. Then use the functional equation $D_F(k) = D_F(q-k_1, k_2, q-k_3, k_4, \ldots, k_s) + (k_1+k_3-q)k_2k_4\cdots k_s$, applied to $k, k+e_1, k+e_2$ and $k+e_1+e_2$. We get $D_{1,2}(k) + D_{1,2}(q-1-k_1, k_2, q-k_3, k_4, \ldots, k_s) = k_4\cdots k_s$. Since $D_{1,2}(q-1-k_1, k_2, q-k_3, k_4, \ldots, k_s) \geq 0$ by the first inequality, $D_{1,2}(k) \leq k_4\cdots k_s$. ■

Proposition 4.9. *If $s \geq 3$ and $k \in I_q^s$, then $|\, l_F(k)\,| \leq q^{s-3}$.*

Proof. Since $l_F(k) = l_F(q-1-k_1, q-1-k_2, k_3, \ldots, k_s)$, we may assume that $0 \leq k_i \leq \frac{q-1}{2}$ for $2 \leq i \leq s$. It easily follows from the definition of $D_{1,2}$ that

$$l_F(k) = (-1)^{s+\Sigma r_i}\Bigg(\sum_{\substack{(\epsilon_3,\ldots,\epsilon_s)\in\{0,1\}^{s-2}\\ \epsilon_3+\cdots+\epsilon_s \text{ even}}} D_{1,2}(k_1, k_2, k_3+\epsilon_3, \ldots, k_s+\epsilon_s)$$

$$- \sum_{\substack{(\epsilon_3,\ldots,\epsilon_s)\in\{0,1\}^{s-2}\\ \epsilon_3+\cdots+\epsilon_s \text{ odd}}} D_{1,2}(k_1, k_2, k_3+\epsilon_3, \ldots, k_s+\epsilon_s)\Bigg).$$

Since $D_{1,2}(k') \geq 0$ for all $k' \in I_\infty^s$,

$$|\, l_F(k)\,| \leq \max\Bigg(\sum_{\epsilon_3+\cdots+\epsilon_s \text{ even}} D_{1,2}(k_1, k_2, k_3+\epsilon_3, \ldots, k_s+\epsilon_s),$$

$$\sum_{\epsilon_3+\cdots+\epsilon_s \text{ odd}} D_{1,2}(k_1, k_2, k_3+\epsilon_3, \ldots, k_s+\epsilon_s)\Bigg).$$

Lemma 4.8 shows then each of these sums is bounded by

$$\sum_{(\epsilon_4,\ldots,\epsilon_s)\in\{0,1\}^{s-3}} (k_4+\epsilon_4)\cdots(k_s+\epsilon_s) = (2k_4+1)\cdots(2k_s+1) \leq q^{s-3}.$$

■

5. Some p - multiplicativity results

Fix an integer $p > 1$. In the applications p is prime but this isn't essential to our formalism. $q \geq 1$ will always denote a power of p.

Definition 5.1. *A function $m : I^s_\infty \to \mathbf{Z}$ is "q - multiplicative" if*

(i) $m(0, \ldots, 0) = 1$.

(ii) Suppose $r \in I^s_\infty$ and $k \in I^s_q$. Set $k^* = (q-1-k_1, k_2, \ldots, k_s)$. Then $m(qr+k) = m(r)m(k)$ if r is even, and is $m(r)m(k^*)$ if r is odd.

Remark 1. When $q = 1$, $k = k^* = (0, \ldots, 0)$. So (ii) follows automatically from (i).

Remark 2. Let $\sigma(r) = 1$ or -1 according as r is even or odd. It is easily seen that σ is q - multiplicative for any q. So $r \mapsto m(r)$ is q - multiplicative if and only if $r \mapsto \sigma(r)m(r)$ is q - multiplicative.

Lemma 5.2. *If m is p - multiplicative, then it is q - multiplicative for any q.*

Proof. We may assume that $q = p^j$ with $j \geq 1$; argue by induction on j. Suppose $j > 1$ and $u = p^j r + k$ with $r \in I^s_\infty$ and $k \in I^s_{p^j}$. Write $k = p^{j-1}a + b$ with $a \in I^s_p$, $b \in I^s_{p^{j-1}}$. Let $a^* = (p-1-a_1, a_2, \ldots, a_s)$, $b^* = (p^{j-1} - 1 - b_1, b_2, \ldots, b_s)$.

Suppose first that r is even. By induction, $m(k) = m(a)m(b)$ or $m(a)m(b^*)$ according as a is even or odd. Also $u = p^{j-1}(pr+a) + b$, and $pr + a$ has the same parity as a. So by induction, $m(u) = m(pr+a)m(b)$ or $m(pr+a)m(b^*)$ according as a is even or odd. Thus $m(u) = m(r)\big(m(a)m(b)\big)$ or $m(r)\big(m(a)m(b^*)\big)$ according as a is even or odd, giving the result.

Suppose next that r is odd and let $k^* = (p^j - 1 - k_1, k_2, \ldots, k_s)$. Then $k^* = p^{j-1}a^* + b^*$. So by induction, $m(k^*) = m(a^*)m(b^*)$ or $m(a^*)m(b)$ according as a^* is even or odd. Now a and a^* have the same parity if p is odd and opposite parity if p is even. It follows that $pr + a$ and a^* have opposite parity. So by induction, $m(u) = m(pr+a)m(b^*)$ or $m(pr+a)m(b)$ according as a^* is even or odd. Since $m(pr+a) = m(r)m(a^*)$, $m(u) = m(r)m(k^*)$, giving the result. ▮

Corollary 5.3. *Let m_0 be a function $I^s_p \to \mathbf{Z}$ with $m(0, \ldots, 0) = 1$. Then m_0 has an extension $m : I^s_\infty \to \mathbf{Z}$ that is q - multiplicative for every q. This extension is unique.*

Proof. Define m inductively, using induction on $\sum r_i$. If $u \in I_p^s$, set $m(u) = m_0(u)$. If $u \notin I_p^s$, we can write $u = pr + k$ with $k \in I_p^s$; set $m(u) = m(r)m(k)$ or $m(r)m(k^*)$ according as r is even or odd. Then m extends m_0 and is p - multiplicative. Now apply Lemma 5.2. Uniqueness is clear. ∎

Suppose now that $s = 3$. We shall show that the function $l_F : I_\infty^3 \to \mathbf{Z}$ of Definition 4.2 is p - multiplicative whenever F is a field of characteristic $p > 0$.

It will be convenient to extend the definition of $[k]_F$ to triples of non-negative integers $k = (k_1, k_2, k_3)$ where the triangle inequalities fail.

Definition 5.4. *If $k_1 > k_2 + k_3$, $[k]_F = \frac{k_1 - k_2 - k_3}{2}$; make similar definitions when $k_2 > k_1 + k_3$ or $k_3 > k_1 + k_2$.*

Remark . Note that $[k]_F \geq 0$, that changing any k_i by 1 changes $[k]_F$ by $\frac{1}{2}$, and that

$$D_F(k) = \frac{2k_1k_2 + 2k_1k_3 + 2k_2k_3 - k_1^2 - k_2^2 - k_3^2}{4} + [k]_F^2$$

in this case as well.

Lemma 5.5.

$$l_F(k) = \sum_{\substack{\epsilon \in \{0,1\}^3 \\ k+\epsilon \text{ odd}}} [k+\epsilon]_F^2 - \sum_{\substack{\epsilon \in \{0,1\}^3 \\ k+\epsilon \text{ even}}} [k+\epsilon]_F^2.$$

Proof. This follows directly from Lemma 2.2 and Proposition 4.3. ∎

Lemma 5.6. *Suppose char$F = 0$. If $k = (k_1, k_2, k_3)$ satisfies the triangle inequalities, then $[k]_F = 0$ or $\frac{1}{2}$ according as k is even or odd.*

Proof. We may assume $k_1 \leq k_2 \leq k_3$. If k is odd, we may reduce to the case of even k by replacing k_3 by $k_3 - 1$ and using Proposition 2.6.

Suppose k is even. Let $R = F[x, y]/(x^{k_1}, y^{k_2})$, α and μ be as in Theorem 2.3 and $\varphi_\mu : R_\mu \to R_{\mu+k_3}$ be induced by multiplication by $(x + y)^{k_3}$. In view of Theorem 2.3, it suffices to show that φ_μ is $1 - 1$. But in Proposition 2.5 we calculated a matrix for φ_μ ; this is the matrix of Definition 2.8 with $k = k_3$, $r = \frac{\alpha}{2}$ and $s = k_3 - k_2$. By Lemma 2.9 the determinant of this matrix is a non-zero integer ; since $\mathbf{Z} \subset \mathbf{F}$, φ_μ is $1 - 1$ and $[k]_F = 0$. ∎

Theorem 5.7. *Suppose char$F = 0$. Then $l_F(k) = 1$ if k satisfies the triangle inequalities and is 0 otherwise.*

Proof. Suppose k satisfies the triangle inequalities. Then each $k + \epsilon$ that is even also satisfies these inequalities. So if $k+\epsilon$ is even, Lemma 5.6 shows that $[k+\epsilon]_F = 0$.

Proposition 2.6 then shows that $[k+\epsilon]_F = \frac{1}{2}$ whenever $k+\epsilon$ is odd, and we apply Lemma 5.5.

If k does not satisfy the triangle inequalities, we may assume $k_1 > k_2+k_3$. Then $D_F(k+\epsilon) = (k_2+\epsilon_2)(k_3+\epsilon_3)$; since the coefficient of $\epsilon_1\epsilon_2\epsilon_3$ in this expression is zero, $l_F(k) = 0$. ∎

From now on F is a field of characteristic $p > 0$.

Lemma 5.8. *Let $k = (k_1, k_2, k_3)$ with $k_i \le p$ and $\sum k_i \le 2p+1$. If k satisfies the triangle inequalities, then $[k]_F = 0$ or $\frac{1}{2}$ according as k is even or odd.*

Proof. We argue precisely as in the proof of Lemma 5.6. We may assume that k is even with $k_1 \le k_2 \le k_3$. Since $k + r - 1 = k_3 + \frac{k_1+k_2-k_3}{2} - 1 < p$, Lemma 2.9 shows that the matrix representing φ_μ has determinant an integer prime to p. So φ_μ is $1-1$ and $[k]_F = 0$. (Alternatively one can use Theorem 2.23.) ∎

Theorem 5.9. *Let $k = (k_1, k_2, k_3)$ with $k_i \le p-1$. If k satisfies the triangle inequalities, and in addition $k_1 + k_2 + k_3 \le 2p-2$, then $l_F(k) = 1$; otherwise $l_F(k) = 0$.*

Proof. The first result is deduced from Lemma 5.8 precisely as Theorem 5.7 is deduced from Lemma 5.6.

If k does not satisfy the triangle inequalities, the proof of Theorem 5.7 shows that $l_F(k) = 0$. Suppose finally that $k_1 + k_2 + k_3 > 2p-2$. By Proposition 4.6, $l_F(k) = l_F(k_1, p-1-k_2, p-1-k_3)$. Since $k_1 > (p-1-k_2)+(p-1-k_3)$, $l_F(k) = 0$. ∎

Definition 5.10. *Suppose $u \in \mathbf{Z}^3$. T_u is the open tetrahedron with vertices at the four even points of the form $u+\epsilon$, $\epsilon \in \{0,1\}^3$.*

Remark . T_u is the tetrahedral cell containing $\left(u_1+\frac{1}{2}, u_2+\frac{1}{2}, u_3+\frac{1}{2}\right)$. T_0 is just the T of Lemma 2.16. Also $T_{(-1-u_1,-1-u_2,-1-u_3)} = -T_{(u_1,u_2,u_3)}$.

Definition 5.11. *u is called "p - special" if for each $j \ge 0$, the cell containing $p^{-j}T_u$ is tetrahedral. (Alternatively, u is p - special if for each $j \ge 0$, the point $p^{-j}\left(u_1+\frac{1}{2}, u_2+\frac{1}{2}, u_3+\frac{1}{2}\right)$ is tetrahedral.)*

Lemma 5.12. *Suppose $u \in I_p^3$. Then $p^{-1}T_u$ is contained either in T_0 or in an octahedral cell. The following are equivalent :*

(i) $u \in (p-1)\overline{T_0}$

(ii) $p^{-1}T_u \subset T_0$

(iii) u *is* p *- special.*

Proof. Let $z_i = p^{-1}(u_i + \frac{1}{2})$. If $u_1 \geq u_2 + u_3 + 1$, $|z_1 - 1| + |z_2| + |z_3| = p^{-1}(p - u_1 + u_2 + u_3 + \frac{1}{2}) < 1$, so z is in the octahedral cell with center $(1,0,0)$ and $p^{-1}T_u$ is contained in this cell. (See Lemma 2.17 (iv).) If $u_1 + u_2 + u_3 \geq 2p - 1$, $|z_1 - 1| + |z_2 - 1| + |z_3 - 1| = p^{-1}(3p - u_1 - u_2 - u_3 - \frac{3}{2}) < 1$, so z (and $p^{-1}T_u$) are in the octahedral cell with center $(1,1,1)$.

Suppose $u \in (p-1)\overline{T_0}$. Since the u_i satisfy the triangle inequalities, the z_i satisfy the strict triangle inequalities. Also $z_1 + z_2 + z_3 \leq p^{-1}\big((2p-2) + \frac{3}{2}\big) < 2$. So z (and $p^{-1}T_u$) are in T_0. We have established the first claim of the lemma and shown that (i) $\Longleftrightarrow$ (ii).

Suppose $p^{-1}T_u \subset T_0$. Then $p^{-j}T_u \subset T_0$ for all $j \geq 1$ and u is p - special. So (ii) $\Rightarrow$ (iii).

Finally suppose u is p - special. Then $p^{-1}T_u$ is contained in a tetrahedral cell which can only be T_0, so (iii) $\Rightarrow$ (ii). ∎

Lemma 5.13. *Suppose $k \in I_p^3$ and $u \in \mathbf{Z}^3$. Then*

(i) $p^{-1}T_{pu+k} \subset T_u$ or an octahedral cell.

(ii) When u is even, $p^{-1}T_{pu+k} \subset T_u$ if and only if k is p - special.

(iii) When u is odd, $p^{-1}T_{pu+k} \subset T_u$ if and only if $(p-1-k_1, p-1-k_2, p-1-k_3)$ is p - special.

Proof. Suppose first that u is even. When $u = (0,0,0)$, (i) and (ii) follow from Lemma 5.12 ; the general case reduces to this by a translation argument.

Suppose next that u is odd. Using a translation argument, we reduce to the case $u = (-1,-1,-1)$. Then $T_u = -T_0$ and $T_{pu+k} = T_{(k_1-p,k_2-p,k_3-p)} = -T_{(p-1-k_1,p-1-k_2,p-1-k_3)}$. So (i) and (iii) follow from Lemma 5.12, with k replaced by $(p-1-k_1, p-1-k_2, p-1-k_3)$. ∎

Lemma 5.14. *Suppose $k \in I_p^3$ and $u \in I_\infty^3$.*

(i) If u is even, $pu + k$ is p - special if and only if u and k are p - special.

(ii) If u is odd, $pu + k$ is p - special if and only if u and $(p-1-k_1, k_2, k_3)$ are p - special.

Proof. First note that $(p-1-k_1, p-1-k_2, p-1-k_3) \in (p-1)\overline{T_0} \Longleftrightarrow$ $(p-1-k_1, k_2, k_3) \in (p-1)\overline{T_0}$.

Suppose that $pu+k$ is p - special. Then $p^{-1}T_{pu+k}$ is contained in a tetrahedral cell. By Lemma 5.13, $p^{-1}T_{pu+k} \subset T_u$, and k is p - special for even u, while $(p-1-k_1, p-1-k_2, p-1-k_3)$ (and consequently $(p-1-k_1, k_2, k_3)$) is p - special for odd u. Furthermore $p^{-j-1}T_{pu+k} \subset p^{-j}T_u$. So $p^{-j}T_u$ and $p^{-j-1}T_{pu+k}$ are contained in the same cell. We conclude that $p^{-j}T_u$ is contained in a tetrahedral cell for all j and that u is p - special.

The proof of the converse results is similar. ∎

To prove the p - multiplicativity of l_F, we shall use Lemma 5.14. We shall also need to show that $l_F(k) = 1$ or 0 according as k is or is not p - special ; the proof of this will be based on the criterion given in Theorem 2.23 for $[k]_F$ to be zero.

Lemma 5.15. $0 \leq D_{i,j}(k) \leq 1$.

Proof. This is immediate from Lemma 4.8. ∎

Lemma 5.16. $D_{i,j}(k) = \frac{1}{2} + [k]_F^2 + [k+e_i+e_j]_F^2 - [k+e_i]_F^2 - [k+e_j]_F^2$.

Proof. This follows directly from Lemma 2.2. ∎

Lemma 5.17. *If k is p - special, $l_F(k) = 1$.*

Proof. Since $p^{-j}T_k \subset T_0$ for large j, the points of T_k satisfy the triangle inequalities. Let z be one of the vertices of T_k. Then for each $j \geq 0$, $p^{-1}z$ is contained in the closure of a tetrahedral cell. Theorem 2.23 then shows that $[z]_F = 0$. So whenever $k + \epsilon$ is even, $[k+\epsilon]_F = 0$. Then whenever $k+\epsilon$ is odd, $[k+\epsilon]_F = \frac{1}{2}$. Lemma 5.5 now shows that $l_F(k) = 1$. ∎

Lemma 5.18. *Suppose k is not p - special. Then there is a vertex z of T_k with $[z]_F \neq 0$.*

Proof. Since k is not p - special, $p^{-j}T_k$ is contained in an octahedral cell C for some j. Let z_1, z_2, z_3, z_4 be the vertices of T_k. Then the $p^{-j}z_i$ are all in the closure of C. Easy geometry shows that they cannot all lie on the boundary of C. So we may assume $p^{-j}z_1$ is octahedral. Now apply Theorem 2.23. (When z_1 does not satisfy the triangle inequalities, the result is trivial.) ∎

Lemma 5.19. *Suppose $[k+e_1]_F = [k+e_2]_F$. Then either $D_{1,2}(k) = 1$ or $[k]_F = [k+e_1+e_2]_F = 0$.*

Proof. By Lemma 5.15, $D_{1,2}(k) = 0$ or 1. So if it is not 1, it must be 0. Let $[k+e_1]_F = [k+e_2]_F = \lambda$. Then by Lemma 5.16 either

(i) $D_{1,2}(k) = \frac{1}{2} + (\lambda + \frac{1}{2})^2 - (\lambda - \frac{1}{2})^2 - 2\lambda^2 = 1$,

(ii) $D_{1,2}(k) = \frac{1}{2} + 2(\lambda + \frac{1}{2})^2 - 2\lambda^2 = 1 + 2\lambda$, or

(iii) $D_{1,2}(k) = \frac{1}{2} + 2(\lambda - \frac{1}{2})^2 - 2\lambda^2 = 1 - 2\lambda$.

So if $D_{1,2}(k) = 0$, we must be in case (iii) with $\lambda = \frac{1}{2}$ and $[k]_F = [k+e_1+e_2]_F = 0$.

∎

Theorem 5.20. *Suppose k is not p - special. Then $l_F(k) = 0$.*

Proof. As in the proof of Proposition 4.9 we see that $(-1)^{k_1+k_2+k_3} l_F(k) = D_{1,2}(k+e_3) - D_{1,2}(k) = D_{1,3}(k+e_2) - D_{1,3}(k) = D_{2,3}(k+e_1) - D_{2,3}(k)$. So if $l_F(k) \neq 0$, Lemma 5.15 shows that either $D_{1,2}(k) = D_{1,3}(k) = D_{2,3}(k) = 0$ or $D_{1,2}(k+e_3) = D_{1,3}(k+e_2) = D_{2,3}(k+e_1) = 0$.

Suppose first that $D_{1,2}(k+e_3) = D_{1,3}(k+e_2) = D_{2,3}(k+e_1) = 0$. Since the $[k+e_i]_F$ all differ from $[k]_F$ by $\frac{1}{2}$, we may assume that $[k+e_1]_F = [k+e_2]_F$. By Lemma 5.19, $[k]_F = 0$. Then each $[k+e_i]_F = \frac{1}{2}$. So by Lemma 5.19 again, each $[k+e_i+e_j]_F = 0$. This contradicts Lemma 5.18.

Suppose now that $D_{1,2}(k+e_3) = D_{1,3}(k+e_2) = D_{2,3}(k+e_1) = 0$. The $[k+e_i+e_j]_F$ all differ from $[k+e_1+e_2+e_3]_F$ by $\frac{1}{2}$. So we may assume that $[k+e_3+e_1]_F = [k+e_3+e_2]_F$. By Lemma 5.19, $[k+e_1+e_2+e_3]_F = 0$. Then each $[k+e_i+e_j]_F = \frac{1}{2}$. So by Lemma 5.19 again, each $[k+e_i]_F = 0$. This once again contradicts Lemma 5.18. ∎

Combining Lemma 5.14 with Theorems 5.17 and 5.20 we get :

Theorem 5.21. *When $s = 3$, the function l_F is p - multiplicative.*

Now suppose that F is a field of characteristic $p = 2$ and that s is arbitrary. We will show that l_F is 2 - multiplicative.

Lemma 5.22. *If $k \in I_q^s$ with exactly one $k_i \geq \frac{q}{2}$, $l_F(k) = 0$.*

Proof. First note that $\frac{q}{2}$ is a power of 2. Let $\epsilon \in \{0,1\}^s$. For $j \neq i$, $k_j + \epsilon_j \leq \frac{q}{2}$, and therefore $D_F(k+\epsilon) = \prod_{j \neq i}(k_j + \epsilon_j)$. Since the coefficient of $\epsilon_1 \cdots \epsilon_s$ in this expression is zero, $l_F(k) = 0$. ∎

Lemma 5.23. *If $k \in \{0,1\}^s$, then $l_F(k) = 1$ or 0 according as k is even or odd.*

Proof. If $\sum k_i \leq 1$, use Lemma 5.22. If $\sum k_i > 1$, use Proposition 4.6 (i) with $q = 2$ and induction. ∎

Theorem 5.24. *Let $k \in \{0,1\}^s$ and $u \in I_\infty^s$. Then $l_F(2u+k) = l_F(u) l_F(k)$.*

Proof. Induction on $\sum u_i$. Choose $q = 2^n$ as small as possible so $u \in I_q^s$. If $q = 1$, then $u = 0$ and the result is trivial. If $q > 1$, at least one $u_i \geq \frac{q}{2}$. If exactly one $u_i \geq \frac{q}{2}$, then exactly one $2u_i + k_i \geq q$. Lemma 5.22 then shows that $l_F(u) = l_F(2u+k) = 0$. If, say, u_1 and u_2 are $\geq \frac{q}{2}$, let $u' = (q-1-u_1, q-1-u_2, u_3, \ldots, u_s)$, $k' = (1-k_1, 1-k_2, k_3, \ldots, k_s)$. By Proposition 4.6 (i) and induction, $l_F(2u+k) = l_F(2u'+k') = l_F(u') l_F(k') = l_F(u) l_(k)$. ∎

Theorem 5.25. *If char$F = 2$, l_F is 2 - multiplicative for every s.*

Proof. Suppose $k \in \{0,1\}^s$. If u is even, Theorem 5.24 shows that $l_F(2u+k) = l_F(u)l_F(k)$. Suppose u is odd. Writing $u = 2a + b$ with $b \in \{0,1\}^s$ and applying Theorem 5.24 and Lemma 5.23, we find that $l_F(u) = l_F(a)l_F(k) = 0$. Furthermore $l_F(2u+k) = l_F(u)l_F(k) = 0$. So $l_F(2u+k)$ and $l_F(u)l_F(1-k_1, k_2, \ldots, k_s)$ are both zero. ▮

6. The D_F - conjecture

p is a prime and F is a field of characteristic p. $q \geq 1$ denotes a power of p.

Definition 6.1.

(i) $m : I_q^s \to \mathbf{Z}$ is q - regular if when any $s-1$ of the variables k_i are fixed, the sum of m over the q values of the remaining variable is 1.

(ii) $m : I_\infty^s \to \mathbf{Z}$ is q - regular if the restriction of m to I_q^s is q - regular.

Lemma 6.2. *If m is p - multiplicative and p - regular, then it is q - regular for every q.*

Proof. It suffices to prove p^j - regularity for $j \geq 1$, and we argue by induction on j. Suppose we fix the last $s-1$ variables. It suffices to show that

$$\sum_{0 \leq r_1 \leq p^{j-1}-1} \sum_{0 \leq k_1 \leq p-1} m(pr+k) = 1$$

whenever $k_2, \ldots, k_s$ are in $[0, p-1]$ and $r_2, \ldots, r_s$ are in $[0, p^{j-1}-1]$.

Fix r_1. If $\sum r_i$ is even, $m(pr+k) = m(r)m(k)$. Using p - regularity we see that the interior sum is $m(r)$. Using p^{j-1} - regularity we see that the double sum is 1. If, on the other hand, $\sum r_i$ is odd, then $m(pr+k) = m(r)m(p-1-k_1, k_2, \ldots, k_s)$. So once again the interior sum is $m(r)$ and the double sum is 1. The argument when $s-1$ variables including the first are fixed is similar. ∎

Corollary 6.3. *If $m_0 : I_p^s \to \mathbf{Z}$ is p - regular with $m_0(0, \ldots, 0) = 1$, then m_0 has an extension $m : I_\infty^s \to \mathbf{Z}$ that is q - multiplicative and q - regular for all q. This extension is unique.*

Proof. This follows from corollary 5.3 and Lemma 6.2. ∎

Example. Suppose $p = 2$. There is a unique 2 - regular function $m_0 : I_2^s \to \mathbf{Z}$ with $m_0(0, \ldots, 0) = 1$. (This function takes each even r to 1 and each odd r to 0.) So there is a unique extension $m : I_\infty^s \to \mathbf{Z}$ that is 2^j - multiplicative and 2^j - regular for all j. Explicitly $m(r) = 1$ if r is a "balanced Nim position" and is 0 otherwise.

Definition 6.4. *Let D be a function $I^s_\infty \to \mathbf{Z}$. D is "p - induced" if there exists a p - multiplicative, p - regular m such that for all r,*

$$D(r) = \sum_{0 \leq k \leq (r_1 - 1, \ldots, r_s - 1)} m(k).$$

We shall say that D is p - induced from m (or that D is p - induced from m_0 where m_0 is the restriction of m to I^s_p).

Remark . It is easy to see that

$$m(r) = (-1)^s \sum_{\epsilon \in \{0,1\}^s} \sigma(\epsilon) D(r + \epsilon).$$

Lemma 6.5. *Define $m_F : I^s_\infty \to \mathbf{Z}$ by*

$$m_F(r) = (-1)^s \sum_{\epsilon \in \{0,1\}^s} \sigma(\epsilon) D_F(r + \epsilon) = \sigma(r) l_F(r).$$

Then

(i)

$$D_F(r) = \sum_{0 \leq k \leq (r_1 - 1, \ldots, r_s - 1)} m_F(k).$$

(ii) m_F is q - regular for every power q of p.

Proof. This follows immediately from Propositions 4.5 and 4.6. ∎

Lemma 6.6. *Fix p and s. Then there is a unique p - induced function $\widetilde{D_F} : I^s_\infty \to \mathbf{Z}$ such that $\widetilde{D_F}(k) = D_F(k)$ whenever each $k_i \leq p$.*

Proof. Define m_F as in Lemma 6.5 and let $\widetilde{m_0}$ be the restriction of m_F to I^s_p. Lemma 6.5 shows that $\widetilde{m_0}$ is p - regular with $\widetilde{m_0}(0) = 1$. Now let $\widetilde{m}$ be the p - multiplicative extension of $\widetilde{m_0}$ and $\widetilde{D_F}$ the function induced from $\widetilde{m}$. (i) of Lemma 6.5 shows that $\widetilde{D_F}$ agrees with D_F when each $r_i \leq p$. ∎

Theorem 6.7. *The following are equivalent :*

(i) D_F is p - induced.

(ii) D_F coincides with $\widetilde{D_F}$.

(iii) m_F is p - multiplicative.

(iv) l_F is p - multiplicative.

Proof. (i) and (ii) are clearly equivalent. Since σ is p - multiplicative, the same is true of (iii) and (iv).

Suppose D_F is p - induced from some m. One sees easily that $m_F(r) = m(r)$ so that m_F is p - multiplicative.

Finally if m_F is p - multiplicative, the fact that it is p - regular combined with (i) of Lemma 6.5 shows that D_F is p - induced. ∎

Definition 6.8. *Let D be a function $I^s_\infty \to \mathbf{Z}$ and $r \in I^s_\infty$. We say D satisfies condition (Φ_r) if there exists an $l_r \in \mathbf{Z}$ and a $\varphi_r \in M_0$ with the following property:*

Suppose q is any power of p and $k = (k_1, \ldots, k_s)$ with $0 \leq k_i \leq q$. Then

(i) If r is even, $D(qr + k) = l_r D(k) + q^{s-1}\varphi_r(q^{-1}k)$.

(ii) If r is odd, $D(qr + k) = l_r D(q - k_1, k_2, \ldots, k_s) + q^{s-1}\varphi_r(q^{-1}k)$.

Remark . If D satisfies (Φ_r), then l_r and φ_r are uniquely determined ; explicitly

$$l_r = (-1)^s \sum_{\epsilon \in \{0,1\}^s} \sigma(\epsilon) D(r + \epsilon).$$

Suppose that $r \in I^s_\infty$ and $a \in I^s_q$; set $a^* = (q-1-a_1, a_2, \ldots, a_s)$. If D satisfies (Φ_r) and (Φ_a), then it also satisfies (Φ_{qr+a}). Furthermore $l_{qr+a} = l_r l_a$ if r is even and $l_r l_{a^*}$ if r is odd.

Theorem 6.9. *Suppose that $D : I^s_\infty \to \mathbf{Z}$ is p - induced. Then D satisfies (Φ_r) for every $r \in I^s_\infty$.*

Proof. Say D is induced from m. We shall derive an explicit formula for $D(qr+k)$ where q is a power of p and each k_i is in $[0, q]$. $D(qr + k)$ is the sum of all the terms $m(u)$ with $0 \leq u_i < qr_i + k_i$. Fix $a = (a_1, \ldots, a_s)$ with $0 \leq a_i \leq r_i$ and let $S(a)$ consist of the sum of all the $m(u)$ for which $u_i = qa_i + b_i$ with $0 \leq b_i < q$ (and $u_i < qr_i + k_i$). Set $n_i = q$ if $a_i < r_i$ and $n_i = k_i$ if $a_i = r_i$. For u_i to be $< qr_i + k_i$, we must have $0 \leq b_i < n_i$. Thus

$$S(a) = \sum_{b_1=0}^{n_1-1} \cdots \sum_{b_s=0}^{n_s-1} m(qa + b).$$

We claim :

Lemma 6.10.

(i) If $a \neq r$,

$$S(a) = q^{s-1} m(a) \prod_{a_i = r_i} \frac{k_i}{q}.$$

(ii) If $a = r$ and r is even, $S(a) = m(r)D(k)$.

(iii) If $a = r$ and r is odd,

$$S(a) = q^{s-1} m(r) \prod_{i=2}^{s} \frac{k_i}{q} - m(r) D(q - k_1, k_2, \ldots, k_s).$$

Proof. Suppose $a \neq r$. Fix an index j with $a_j < r_j$. Fix b_i for all $i \neq j$ with $0 \leq b_i \leq n_i - 1$. Then for each choice of b_j, $m(qa + b) = m(a)m(b)$ or $m(a)m(q - 1 - b_1, b_2, \ldots, b_s)$ according as a is even or odd ; summing over the $n_j = q$ values of b_j, we find that the partial sum we get is $m(a)$, since m is q - regular. Thus

$$S(a) = m(a) \prod_{i \neq j} n_i = m(a) q^{s-1} \prod_{i=1}^{s} \frac{n_i}{q} = m(a) q^{s-1} \prod_{a_i = r_i} \frac{k_i}{q},$$

giving (i).

Suppose that $a = r$ and r is even. Then

$$S(a) = \sum_{b_1=0}^{k_1-1} \cdots \sum_{b_s=0}^{k_s-1} m(r)m(b) = m(r)D(k).$$

Suppose finally that $a = r$ and r is odd. Then

$$S(a) = \sum_{b_1=0}^{k_1-1} \cdots \sum_{b_s=0}^{k_s-1} m(r)m(q - 1 - b_1, b_2, \ldots, b_s) = \sum_{b_1=q-k_1}^{q-1} \sum_{b_2=0}^{k_2-1} \cdots \sum_{b_s=0}^{k_s-1} m(r)m(b).$$

Write the outer sum as $\sum_{b_1=0}^{q-1} - \sum_{b_1=0}^{q-k_1-1}$. Then $S(a)$ is represented as a difference of two terms. Since m is q - regular, the first term is

$$m(r) \prod_{i=2}^{s} k_i = m(r) q^{s-1} \prod_{i=2}^{2} \frac{k_i}{q},$$

while the second term is evidently $m(r)D(q - k_1, k_2, \ldots, k_s)$. ∎

Since $D(qr + k) = \sum_a S(a)$, (Φ_r) follows immediately from Lemma 6.10 ; note that $l_r = m(r)$ or $-m(r)$ according as r is even or odd. ∎

Theorem 6.11. *The following conditions on D_F are equivalent :*

(i) D_F is p - induced.

(ii) D_F satisfies (Φ_r) for every $r \in I^s_\infty$.

(iii) D_F satisfies (Φ_r) for every $r \in I^s_p$.

Proof. Theorem 6.9 shows that (i) $\Rightarrow$ (ii). (ii) $\Rightarrow$ (iii) is trivial. Suppose finally that (iii) holds. According to the remark after Definition 6.8, D_F satisfies (Φ_r) for all r, the function $r \mapsto l_r$ is p - multiplicative and

$$l_r = (-1)^s \sigma(r) \sum_{\epsilon \in \{0,1\}^s} \sigma(\epsilon) D_F(r+\epsilon) = \sigma(r) m_F(r) = l_F(r).$$

So l_F is p - multiplicative and we apply Theorem 6.7 to get (i). ∎

We can now state the "D_F - conjecture".

Conjecture. *Let F be a field of characteristic p and s an integer ≥ 1. Then the equivalent conditions of Theorems 6.7 and 6.11 are satisfied.*

There are four cases in which the D_F - conjecture is known to hold ; the first two are trivial, the last two are results of chapter 5 (see Theorem 5.9, Theorem 5.21, Lemma 5.23 and Theorem 5.25).

(i) If $s = 1$, then $D_F(r) = \min(r,1)$, $l_F(r) = m_F(r) = \delta_{r,0}$ and D_F is p - induced.

(ii) If $s = 2$, then $D_F(r_1,r_2) = \min(r_1,r_2)$, $l_F(r_1,r_2) = m_F(r_1,r_2) = \delta_{r_1,r_2}$ and D_F is p - induced.

(iii) If $s = 3$ and $r \in I_p^s$, then $l_F(r) = 1$ if r is in the closed tetrahedron with vertices at $(0,0,0)$, $(p-1,p-1,0)$, $(p-1,0,p-1)$ and $(0,p-1,p-1)$, and is 0 otherwise. Furthermore D_F is p - induced.

(iv) If $p = 2$ and $r \in I_2^s$, then $l_F(r) = m_F(r) = 1$ or 0 according as r is even or odd. Furthermore D_F is 2 - induced. (So $D_F(r)$ is the number of balanced Nim positions k with $0 \leq k_i \leq r_i$; see the example after Corollary 6.3.)

We conclude this chapter by developing some properties of $\widetilde{D_F}$ that lend plausibility to the D_F - conjecture for arbitrary p and s.

Lemma 6.12. *Suppose $m_0 : I_p^s \to \mathbf{Z}$ $(s \geq 2)$ satisfies the following conditions : $m_0(0) = 1$, m_0 is a symmetric function of the k_i and $m_0(k) = m_0(p-1-k_1, p-1-k_2, k_3, \ldots, k_s)$.*

Let m be the p - multiplicative extension of m_0. Then m is a symmetric function of the k_i. Furthermore if $k \in I_q^s$, then $m(k) = m(q-1-k_1, q-1-k_2, k_3, \ldots, k_s)$.

Proof. Although m_0 is symmetric, the inductive definition of m in Corollary 5.3 singles out the first variable. But under our hypotheses $m_0(p-1-k_1, k_2, \ldots, k_s) = m_0(k_1, \ldots, p-1-k_i, \ldots, k_s)$. So the dependence on the first variable is only apparent and m like m_0 is symmetric.

To prove the last assertion we write $q = p^j$ and $k = pa + b$ with $a \in I_{p^{j-1}}^s$ and $b \in I_p^s$. The argument, by induction on j, is straitforward. ∎

Theorem 6.13.

(i) $\widetilde{D_F}(qr) = q^{s-1}\widetilde{D_F}(r)$.

(ii) $\widetilde{D_F}$ *is symmetric.*

(iii) If each $r_i \le q$, $\widetilde{D_F}(r) = \widetilde{D_F}(q-r_1, q-r_2, r_3, \dots, r_s) + (r_1+r_2-q)r_3\cdots r_s$.

(iv) If $k_2,\dots,k_s \le q$, *then* $\widetilde{D_F}(q+u_1, k_2, \dots, k_s) = k_2\cdots k_s$.

(v) If $k_3,\dots,k_s \le q$, *then* $\widetilde{D_F}(q+u_1, q+u_2, k_3, \dots, k_s) = \widetilde{D_F}(u_1, u_2, k_3, \dots, k_s) + qk_3\cdots k_s$.

Remark . The above results also hold when $\widetilde{D_F}$ is replaced by D_F ; see Propositions 1.4 and 1.6 and Theorem 3.8.

Proof. Let $\widetilde{m_0}$ be the restriction of m_F to I_p^s and $\widetilde{m}$ the p - multiplicative extension of $\widetilde{m_0}$.

(i) We argue as in the proof of Theorem 6.9 with each $k_i = 0$. Then $\widetilde{D_F}(qr)$ is a sum of terms $S(a)$; since each $k_i = 0$, we may assume that $0 \le a_i < r_i$. By Lemma 6.10, $S(a) = q^{s-1}\widetilde{m}(a)$; summing over a, we get (i).

(ii) Since $\widetilde{m_0}$ is symmetric and by Proposition 4.6 $\widetilde{m_0}(k) = \widetilde{m_0}(p-1-k_1, p-1-k_2, k_3, \dots, k_s)$, Lemma 6.12 shows that $\widetilde{m}$ is also symmetric.

(iii) Lemma 6.12 also shows that if $k \in I_q^s$, $\widetilde{m}(k) = \widetilde{m}(q-1-k_1, q-1-k_2, k_3, \dots, k_s)$. Using this fact and the q - regularity of $\widetilde{m}$, it is easy to deduce (iii).

(iv) Write $q+u_1 = cq+k_1$ with $0 \le k_1 \le q-1$. We use the argument of Theorem 6.9 to calculate $\widetilde{D_F}(cq+k_1, k_2, \dots, k_s)$. Since $m_F(a, 0, \dots, 0) = \delta_{a,0}$, $\widetilde{m}(a, 0, \dots, 0) = \delta_{a,0}$. Thus the only non-vanishing $S(a)$ is $S(0) = q^{s-1}\prod_2^s \frac{k_i}{q} = k_2\cdots k_s$.

(v) Let $u_1 = r_1q + k_1$, $u_2 = r_2q + k_2$ with $0 \le k_1, k_2 \le q-1$ and use the argument of Theorem 6.9 to calculate $\widetilde{D_F}(r_1q+k_1, r_2q+k_2, k_3, \dots, k_s)$. Note that $m_F(a, b, 0, \dots, 0) = \delta_{a,b}$ and an easy induction shows that $\widetilde{m}(a, b, 0, \dots, 0) = \delta_{a,b}$. So the only non-vanishing $S(a)$ are those with $a = (x, x, 0, \dots, 0)$, $\quad x \le \min(r_1, r_2)$. If $x < \min(r_1, r_2)$, the corresponding $S(a)$ is $q^{s-1}\prod_2^s \frac{k_i}{q} = qk_3\cdots k_s$. If $x = \min(r_1, r_2)$, the corresponding $S(a)$ is $k_2k_3\cdots k_s$, $D_F(k_1, \dots, k_s)$ or $k_1k_3\cdots k_s$ according as $r_1 > r_2$, $r_1 = r_2$ or $r_1 < r_2$. The effect of replacing r_1 by r_1+1 and r_2 by r_2+1 is thus to add one additional $S(a)$ of the form $qk_3\cdots k_s$, giving (v). ∎

7. Applications of the D_F - conjecture to Hilbert - Kunz functions

Throughout this section p is a fixed prime ; q is always a power of p. $D : I^s_\infty \to \mathbf{Z}$ is a p - induced function in the sense of Definition 6.4.

Definition 7.1. *If $r \in I^s_\infty$,*

$$m(r) = (-1)^s \sum_{\epsilon \in \{0,1\}^s} \sigma(\epsilon) D(r+\epsilon)$$

and $l(r) = \sigma(r)m(r)$.

Remark . m and l are p - multiplicative and D satisfies condition (Φ_r) with $l_r = l(r)$.

Lemma 7.2. *Suppose that $r \in I^s_\infty$, $k \in I^s_q$ and $z \in [0,1]^s$.*

(i) If r is even,

$$\varphi_{qr+k}(z) = l_r \varphi_k(z) + q^{s-1}\varphi_r\left(\frac{k+z}{q}\right).$$

(ii) If r is odd, set $k^* = (q-1-k_1, k_2, \ldots, k_s)$. Then

$$\varphi_{qr+k}(z) = l_r \varphi_{k^*}(1-z_1, z_2, \ldots, z_s) + q^{s-1}\varphi_r\left(\frac{k+z}{q}\right).$$

Proof. It suffices to prove the lemma when the z_i are replaced by indeterminates, t_i.

Suppose first that $qr+k$ is even. Adopt the language of Definition 4.1. Both sides of the two identities to be proved are elements of M_0. Using the remark after Definition 4.1 we see that it is enough to prove (i) and (ii) when z is an element ϵ of $\{0,1\}^s$, and that we may even assume that $\epsilon \neq (1,\ldots,1)$, so that $D(\epsilon) = 0$. Since $qr+k$ is even, either r and k are both even or r is odd and k^* is odd. In both cases $D(qr+k+\epsilon) = \varphi_{qr+k}(\epsilon)$. Furthermore D satisfies (Φ_r). So in the first case $D\big(qr+(k+\epsilon)\big) = l_r D(k+\epsilon) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right) = l_r\varphi_k(\epsilon) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right)$, while in the second case it is $l_r D\big((q-1-k_1)+(1-\epsilon_1), k_2+\epsilon_2, \ldots, k_s+\epsilon_s\big) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right) = l_r\varphi_{k^*}(1-\epsilon_1, \epsilon_2, \ldots, \epsilon_s) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right)$.

$D(1-\epsilon_1,\epsilon_2,\ldots,\epsilon_s) = 0$. Now either r is even and k odd or r is odd and k^* even. In both cases $D(qr+k+\epsilon) = \varphi_{qr+k}(\epsilon)$. In the first case $D\big(qr+(k+\epsilon)\big) = l_r D(k+\epsilon) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right) = l_r\varphi_k(\epsilon) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right)$, while in the second case it once again is $l_r D\big((q-1-k_1)+(1-\epsilon_1), k_2+\epsilon_2,\ldots,k_s+\epsilon_s\big) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right) = l_r\varphi_{k^*}(1-\epsilon_1,\epsilon_2,\ldots,\epsilon_s) + q^{s-1}\varphi_r\left(\frac{k+\epsilon}{q}\right)$. ∎

Definition 7.3. *If $u \in I^s_\infty$, let G_u be the unique element of M whose value at any $\epsilon \in \{0,1\}^s$ is $D(u+\epsilon)$. Explicitly*

$$G_u(z) = \sum_{\epsilon\in\{0,1\}^s}\left(\prod_{\epsilon_i=1} z_i\right)\left(\prod_{\epsilon_i=0}(1-z_i)\right)D(u+\epsilon).$$

Definition 7.4. *If $\beta \in [0,\infty)^s$, let u (or more precisely $u(\beta)$) be the element $([\beta_1],\ldots,[\beta_s])$ of I^s_∞ and z (or more precisely $z(\beta)$) be $\beta - u$. Set $g(\beta) = G_u(z)$ where $u = u(\beta)$, $z = z(\beta)$.*

Remark 1. If $\beta \in I^s_\infty$, $g(\beta) = G_\beta(0) = D(\beta)$. So g is an extension of D to $[0,\infty)^s$. (It is a kind of piecewise linear interpolation of D.)

Remark 2. G_u is closely related to φ_u. In fact $\varphi_u(z) = G_u(z) - l_u z_1\cdots z_s$ or $G_u(z) - l_u(1-z_1)z_2\cdots z_s$ according as u is even or odd.

Remark 3. Let $d_1,\ldots,d_s$ be positive integers and $\beta = \left(\frac{1}{d_1},\ldots,\frac{1}{d_s}\right)$. If $n \geq 0$, write $p^n = d_i u_i + a_i$ with $0 \leq a_i < d_i$. Then $u(p^n\beta) = (u_1,\ldots,u_s)$ and $z(p^n\beta) = \left(\frac{a_1}{d_1},\ldots,\frac{a_s}{d_s}\right)$. Using the formula for G_u in Definition 7.3, we find that

$$d_1\cdots d_s g(p^n\beta) = \sum_{\epsilon\in\{0,1\}^s}\left(\prod_{\epsilon_i=1} a_i\right)\left(\prod_{\epsilon_i=0}(d_i-a_i)\right)D(u_1+\epsilon_1,\ldots,u_s+\epsilon_s).$$

Suppose now that $F = \mathbf{Z}/p$, that $D = D_F$ (and that the D_F - conjecture holds). Then by Proposition 1.3 this last sum is just e_n, the F - dimension of

$$F[[x_1,\ldots,x_s]]/(\sum_1^s x_i^{d_i}, x_1^{p^n},\ldots,x_s^{p^n}).$$

So the problem of describing e_n as a function of n is just the problem of describing $g(p^n\beta)$ as a function of n.

Motivated by the last remark, we shall consider the following problem. Let D be any p - induced function and $\beta \in [0,\infty)^s$ where each β_i is rational. How does $g(p^j\beta)$ depend on β? We shall prove :

Theorem 7.5. *Suppose D satisfies the following condition : if $t \in I_q^s$ then $l_t \neq q^{s-1}$. Let $\beta = (\beta_1, \ldots, \beta_s)$ where the β_i are non-negative and rational. Then there is a rational C and integers $l^{\#}$ and λ, $\lambda \geq 1$, such that :*
(i) $g(p^j\beta) = Cp^{(s-1)j} + \Delta_j$ where
(ii) $\Delta_{j+\lambda} = l^{\#}\Delta_j$ for all large j.

Theorem 7.5 evidently holds for β if and only if it holds for $p\beta$. So multiplying β by a power of p we may assume that the β_i have denominators prime to p ; when p is even we may further assume that $\sum \beta_i$ has even denominator. Choose $\lambda \geq 1$ so that $(p^\lambda - 1)\beta$, and consequently $(p^\lambda - 1)z$ are in I_∞^s. When p is odd, we may further assume that $(p^\lambda - 1)z$ is even (replace λ by 2λ if necessary). So we only need to prove Theorem 7.5 in the situation of the following definition.

Definition 7.6. *Henceforth $\beta = (\beta_1, \ldots, \beta_s)$ where the β_i are non-negative rational numbers with denominators prime to p ; when p is even, we assume that $\sum \beta_i$ has even numerator. $u = u(\beta)$, $z = z(\beta)$ and $\lambda \geq 1$ is chosen so that $t = (p^\lambda - 1)z \in I_\infty^s$; if p is odd we further choose λ so that t is even.*

Definition 7.7. *$z^* = (1 - z_1, z_2, \ldots, z_s)$ and $t^* = (p^\lambda - 1)z^*$.*

Definition 7.8. *$z^{\#} = z$ or z^* according as u is even or odd, and $t^{\#} = (p^\lambda - 1)z^{\#}$.*

Remark 1. The coordinates of t, t^* and $t^{\#}$ are integers in $[0, p^\lambda - 1]$. Note that $t_1^* = p^\lambda - 1 - t_1$, while $t_i^* = t_i$ for $i > 1$. So t and t^* have the same parity if p is odd and opposite parity if p is even. In particular, when p is odd, t, t^* and $t^{\#}$ are all even.

Remark 2. Suppose p is even. Since $\sum \beta_i$ has even numerator, $(p^\lambda - 1)\beta$ is even. Then u has the same parity as $(p^\lambda - 1)u = (p^\lambda - 1)\beta - t$, and u and t have the same parity. So if u is even, $t^{\#} = t$ and is even, while if u is odd, $t^{\#} = t^*$ and again is even.

We shall prove the following precise form of Theorem 7.5 :

Theorem 7.5′. *Let β and λ be as in Definition 7.6 and $t^{\#}$ be as in Definition 7.8. Suppose $l_{t^{\#}} \neq p^{\lambda(s-1)}$. Then there is a rational C such that :*
(i) $g(p^j\beta) = Cp^{(s-1)j} + \Delta_j$ where
(ii) $\Delta_{j+\lambda} = l_{t^{\#}}\Delta_j$ for all $j \geq 0$.

Definition 7.9. *Write $p^n z = v_n + z_n$ with $z_n \in [0,1)^s$ and $v_n \in I_\infty^s$. Let z_n^* be obtained from z_n in the same way z^* is obtained from z, and set $z_n^{\#} = z_n$ or z_n^* according as u is even or odd. Let v_n^* is defined so that v_n and v_n^* agree in all coordinates but the first, and have first coordinates summing to $p^n - 1$. Set $v_n^{\#} = v_n$ or v_n^* according as u is even or odd.*

Lemma 7.10.

(i) $z_{n+\lambda} = z_n$, $v_{n+\lambda} = p^n t + v_n$

(ii) $p^n \beta = p^n u + v_n + z_n$

(iii) $p^{n+\lambda}\beta = p^n(p^\lambda u + t) + v_n + z_n$

(iv) u *and* $p^\lambda u + t$ *have the same parity.*

Proof. $p^{n+\lambda}z = p^n(t+z) = p^n t + v_n + z_n$ giving (i). The fact that $\beta = u + z$ then gives (ii) and (iii). The remarks after Definition 7.8 give (iv). ∎

Definition 7.11. *Let* $l^{\#} = l_{t^{\#}}$ and $Q = p^{\lambda(s-1)}$. *Set* $A = \varphi_{p^\lambda u+t}(z) - l^{\#}\varphi_u(z)$.

Remark . Since the coordinates of z are rational, A is rational. Also $p^{-\lambda}(t + z) = z$. So if we apply Lemma 7.2 we get an alternative description of A ; $A = l_u\varphi_{t^{\#}}(z^{\#}) + (Q - l^{\#})\varphi_u(z)$.

Theorem 7.12. $g(p^{n+\lambda}\beta) - l^{\#}g(p^n\beta) = Ap^{n(s-1)}$. *(Here A is the A of Definition 7.11, which is independent of n.)*

Proof. Let Π be the product of the coordinates of z_n or of z_n^* according as $p^n u + v_n$ is even or odd. Then $g(p^n\beta) = \varphi_{p^n u+v_n}(z_n) + l_u l_{v_n^{\#}}\Pi$. Now (iv) of Lemma 7.10 shows that $p^n u + v_n$ and $p^n(p^\lambda u + t) + v_n$ have the same parity. Using (iii) of that lemma we find that $g(p^{n+\lambda}\beta) = \varphi_{p^n(p^\lambda u+t)+v_n}(z_n) + l_u l^{\#} l_{v_n^{\#}}\Pi$ for the same Π. Thus $g(p^{n+\lambda}\beta) - l^{\#}g(p^n\beta) = \varphi_{p^n(p^\lambda+t)+v_n}(z_n) - l^{\#}\varphi_{p^n u+v_n}(z_n)$. Lemma 7.2 shows that the first term is $l_u l^{\#}\varphi_{v_n^{\#}}(z_n^{\#}) + p^{n(s-1)}\varphi_{p^\lambda u+t}(z)$, since $\frac{v_n+z_n}{p^n} = z$. Similarly, the second term is $-l^{\#}\left(l_u\varphi_{v_n^{\#}}(z_n^{\#}) + p^{n(s-1)}\varphi_u(z)\right)$. The theorem follows immediately.

∎

It is now easy to prove Theorem 7.5′. Under the hypotheses of that theorem, $l^{\#} \neq Q$. Set $C = A/(Q - l^{\#})$ and $\Delta_n = g(p^n\beta) - Cp^{n(s-1)}$. Then $\Delta_{n+\lambda} - l^{\#}\Delta_n = Ap^{n(s-1)} - Cp^{n(s-1)}(p^{\lambda(s-1)} - l^{\#}) = 0$, the desired result. ∎

We next apply Theorem 7.5 to Hilbert - Kunz functions. Let p be a prime and $F = \mathbf{Z}/p$. Let $d_1, \ldots, d_s$ and n be integers with $d_i \geq 1$, $n \geq 0$. Set

$$e_n(d_1, \ldots, d_s\,;\, p) = \dim F[[x_1, \ldots, x_s]]/(\sum_1^s x_i^{d_i}, x_1^{p^n}, \ldots, x_s^{p^n}).$$

By Remark 3 following Definition 7.4,

$$e_n(d_1, \ldots, d_s\,;\, p) = d_1 \cdots d_s g\left(\frac{p^n}{d_1}, \ldots, \frac{p^n}{d_s}\right)$$

with $D = D_F$ and g as in Definition 7.4, provided that D_F is p - induced.

Theorem 7.13. *If either $s = 3$ or $p = 2$, $e_n(d_1, \ldots, d_s\,; p) = cp^{(s-1)n} +$ (an eventually periodic function of n), where c is a positive rational.*

Proof. Let $\beta = \left(\frac{1}{d_1}, \ldots, \frac{1}{d_s}\right)$. Then $e_n(d_1, \ldots, d_s\,; p) = d_1 \cdots d_s g(p^n\beta)$ with $D = D_F$ and g as in Definition 7.4. (Note that D_F is p - induced ; see the remarks following the proof of Theorem 6.11.) Furthermore we have shown in Lemma 5.17, Theorem 5.20 and Lemma 5.23 that if $t \in I^s_\infty$, then $l_t = 0$ or 1. Now apply Theorem 7.5, noting that the $l^\#$ of that theorem is just $l_{t^\#}$ for some $t^\# \in I^s_\infty$. ∎

Theorem 7.14. *Suppose $s > 3$ and $D_F : I^s_\infty \to \mathbf{Z}$ is p - induced. Then*

$$e_n(d_1, \ldots, d_s\,; p) = cp^{(s-1)n} + \Delta_n,$$

where c is a positive rational and $\Delta_n = O(p^{(s-3)n})$. Furthermore there are integers λ and $l^\#$ with $\lambda \geq 1$ such that $\Delta_{n+\lambda} = l^\#\Delta_n$ for large enough n.

Proof. Let $\beta = \left(\frac{p^i}{d_1}, \ldots, \frac{p^i}{d_s}\right)$ with i fixed and large. Then $e_n(d_1, \ldots, d_s\,; p) = d_1 \cdots d_s g(p^{n-i}\beta)$ with $D = D_F$ and g as in Definition 7.4. Now choose λ as in Definition 7.8. By Proposition 4.9, $|l_{t^\#}| \leq p^{\lambda(s-3)}$. So the conclusions of Theorem 7.5′ hold, and the theorem follows immediately. ∎

Shortly after we completed this thesis, Monsky discovered that an argument using a representation ring enables one to deduce the p - multiplicativity of l_F for all s from the p - multiplicativity when $s = 3$. He presents this argument in an appendix attached to this thesis. It follows that D_F is p - induced for all s, and we get :

Theorem 7.15. *The conclusions of Theorem 7.14 hold unconditionally.*

In certain cases Theorem 7.5′ can be given a more explicit form.

Theorem 7.16. *Suppose $\beta \in [0, \infty)^s$ and $l_{u(\beta)} = 0$. Then, for all $n > 0$, $l_{u(p^n\beta)} = 0$ and $g(p^n\beta) = p^{(s-1)n}g(\beta)$.*

Proof. Suppose $n = 1$. Write $\beta = u + z$ with $u = u(\beta)$ and $z \in [0, 1)^s$. Write $pz = v + z'$ with $v \in I^s_p$ and $z' \in [0, 1)^s$. Then $p\beta = (pu + v) + z'$, and $l_{u(p\beta)} = l_{pu+v} = 0$. Thus $g(p\beta) = G_{pu+v}(z') = \varphi_{pu+v}(z')$. By Lemma 7.2 this is $p^{s-1}\varphi_u(z) = p^{s-1}G_u(z) = p^{s-1}g(\beta)$. For arbitrary n use induction. ∎

Corollary 7.17. *Suppose we are in the situation of Definition 7.6. If $l_u = 0$, the Δ_j of Theorem 7.5′ is 0 for all $j \geq 0$. If $l^\# = 0$, the Δ_j of Theorem 7.5′ is 0 for all $j \geq \lambda$.*

Proof. The first result follows from Theorem 7.16, and the second from Theorem 7.5′ itself. ∎

Suppose now that we are in the situation of Definition 7.6 with $s = 3$ and $D = D_F$ and seek an explicit formula for the Δ_j of Theorem 7.5′. In view of Corollary 7.17 we only need consider the case $l^\# = l_u = 1$. Furthermore we only need calculate Δ_j for $0 \leq j < \lambda$.

Lemma 7.18. *For $0 \leq j \leq \lambda$ we have $l_{u(p^j\beta)} = 1$.*

Proof. $p^\lambda\beta = p^\lambda u + t + z$. Thus the value of l at $u(p^\lambda\beta)$ is $l_u l^\# = 1$. Now the proof of Theorem 7.16 shows that if $l = 0$ at $u(p^n\beta)$ then $l = 0$ at $u(p^{n+1}\beta)$, giving the lemma. ∎

Lemma 7.19. *Let $H(T_1, T_2, T_3) = T_1T_2 - \left(\frac{T_1+T_2+T_3}{2}\right)^2$. Suppose that $u \in I^3_\infty$ is p - special and ϵ is in $\{0,1\}^3$. Then*

(i) If u is even, $D_F(u+\epsilon) = H(u+\epsilon) - H(\epsilon) + \epsilon_1\epsilon_2\epsilon_3$.

(ii) If u is odd, $D_F(u+\epsilon) = H(u+\epsilon) - H(1-\epsilon_1, \epsilon_2, \epsilon_3) + (1-\epsilon_1)\epsilon_2\epsilon_3$.

Proof. In the situation of (i), $D_F(u+\epsilon) = D_F(u+\epsilon) - D_F(\epsilon) + \epsilon_1\epsilon_2\epsilon_3 = \big(H(u+\epsilon) + [u+\epsilon]_F^2\big) - \big(H(\epsilon) + [\epsilon]_F^2\big) + \epsilon_1\epsilon_2\epsilon_3$. But since u is p - special and even, the proof of Lemma 5.17 shows that $[u+\epsilon]_F = [\epsilon]_F$, giving the result. When u is odd, the argument is similar, using the fact that $[u+\epsilon]_F = [1-\epsilon_1, \epsilon_2, \epsilon_3]_F$. ∎

Lemma 7.20. *Suppose that $\beta = u + z$ with $l_u = 1$ and $z \in [0,1)^3$; write $z = (z^{(1)}, z^{(2)}, z^{(3)})$. Then*

(i) If u is even, $g(\beta) = H(\beta) - H(z) + z^{(1)}z^{(2)}z^{(3)}$.

(ii) If u is odd, $g(\beta) = H(\beta) - H(1-z^{(1)}, z^{(2)}, z^{(3)}) + (1-z^{(1)})z^{(2)}z^{(3)}$.

Proof. Suppose u is even. Theorem 5.20 shows that u is p - special. The polynomial $H(T+u) - H(T) + T_1T_2T_3$ is easily seen to be in M. By Lemma 7.19 its value at any ϵ in $\{0,1\}^3$ is $D_F(u+\epsilon)$. So $H(T+u) - H(T) + T_1T_2T_3 = G_u(T)$. Evaluating at $T_i = z^{(i)}$ we get (i). The proof of (ii) is similar, using the fact that $H(T+u) - H(1-T_1, T_2, T_3) + (1-T_1)T_2T_3$ is in M. ∎

Definition 7.21. *Suppose $\alpha \in [0,1]^3$. Set $H'(\alpha) = \alpha_1\alpha_2\alpha_3 - H(\alpha)$ and $H''(\alpha) = H'(1-\alpha_1, \alpha_2, \alpha_3)$.*

Theorem 7.22. *Suppose that we are in the situation of Definition 7.6 with $s = 3$, $D = D_F$ and $l^\# = l_u = 1$. Write $p^n\beta = u(p^n\beta) + z_n$ with $z_n \in [0,1)^3$. Then*

(i) The constant C of Theorem 7.5′ is $H(\beta)$.

Theorem 7.22. *Suppose that we are in the situation of Definition 7.6 with $s = 3$, $D = D_F$ and $l^{\#} = l_u = 1$. Write $p^n\beta = u(p^n\beta) + z_n$ with $z_n \in [0,1)^3$. Then*

(i) The constant C of Theorem 7.5′ is $H(\beta)$.

(ii) Suppose $0 \le n \le \lambda$. Then the Δ_n of Theorem 7.5′ is $H'(z_n)$ or $H''(z_n)$ according as $u(p^n\beta)$ is even or odd.

Proof. By Lemma 7.18, $l_{u(p^n\beta)} = 1$. The proof of Lemma 7.20 applied to $p^n\beta$ shows that $g(p^n\beta) = H(p^n\beta) + H'(z_n) = p^{2n}H(\beta) + H'(z_n)$ or $p^{2n}H(\beta) + H''(z_n)$ according as $u(p^n\beta)$ is even or odd. Taking $n = 0$ and λ, using the fact that $\Delta_0 = \Delta_\lambda$ and that $u(\beta)$ and $u(p^\lambda\beta)$ have the same parity we find that $C = H(\beta)$. (ii) follows immediately. ∎

Example 1. We shall first calculate $e_n = e_n(5,8,8\,;3)$.

If $\beta = (\frac{1}{5},\frac{1}{8},\frac{1}{8})$, then $3\beta = (\frac{3}{5},\frac{3}{8},\frac{3}{8})$, $9\beta = (1,1,1)+(\frac{4}{5},\frac{1}{8},\frac{1}{8})$, $27\beta = (5,3,3)+(\frac{2}{5},\frac{3}{8},\frac{3}{8})$ and $81\beta = (16,10,10)+\beta$. So we are in the situation of Definition 7.6 with $\lambda = 4$, $u = 0$ and $t^{\#} = t = (16,10,10)$. Since $t^{\#} = 9(1,1,1)+(7,1,1)$, $l^{\#} = l_{t^{\#}} = l_{(1,1,1)}l_{(8-7,1,1)} = l^2_{(1,1,1)}$. But $l_{(1,1,1)} = 1$ by Theorem 5.9. Therefore $l^{\#} = 1$. Since $l_u = 1$, we can apply Theorem 7.22 to calculate C and Δ_n of Theorem 7.5′. Then C is $H(\beta) = \frac{3}{200}$, and $\Delta_0 = H'(\beta) = -\frac{19}{1600}$, $\Delta_1 = H'((\frac{3}{5},\frac{3}{8},\frac{3}{8})) = -\frac{81}{1600}$, $\Delta_2 = H''((\frac{4}{5},\frac{1}{8},\frac{1}{8})) = H'(\beta) = \Delta_0 = -\frac{19}{1600}$ and $\Delta_3 = H''((\frac{2}{5},\frac{3}{8},\frac{3}{8})) = H'((\frac{3}{5},\frac{3}{8},\frac{3}{8})) = \Delta_1 = -\frac{81}{1600}$.

Now $e_n = 320g(p^n\beta)$; by Theorem 7.5′ this is $\frac{24}{5}3^{2n} + 320\Delta_n$ with $\Delta_{n+4} = \Delta_n$ for all n. But we have $\Delta_0 = \Delta_2 = -\frac{19}{1600}$ and $\Delta_1 = \Delta_3 = -\frac{81}{1600}$. Thus $e_n = \frac{24}{5}3^{2n} - \frac{19}{5}$ or $\frac{24}{5}3^{2n} - \frac{81}{5}$ according as n is even or odd.

Example 2. We shall next calculate $e_n = e_n(4,4,4,4\,;5)$.

If $\beta = (\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$, then $5\beta = (1,1,1,1)+\beta$ and we are in the situation of Definition 7.6 with $\lambda = 1$, $u = 0$ and $t^{\#} = t = (1,1,1,1)$. Since $l_u = 1$ and $\varphi_u = 0$, the remark after Definition 7.11 shows that the C appearing there is $\frac{A}{5^3 - l^{\#}}$. By Proposition 4.3, $l^{\#} = \sum_{\epsilon\in\{0,1\}^4}(-1)^{\Sigma\epsilon_i}D_F(t+\epsilon)$. Since $D_F(1,1,1,1) = D_F(2,1,1,1) = 1$, $D_F(2,2,1,1) = 2$, $D_F(2,2,2,1) = 3$ and $D_F(2,2,2,2) = 6$, we get $l^{\#} = 3$. Similarly $\varphi_t(z) = \sum_{\epsilon\in\{0,1\}^4}\left(\prod_{\epsilon_i=1} z_i\right)\left(\prod_{\epsilon_i=0}(1-z_i)\right)D_F(t+\epsilon) - 3z_1z_2z_3z_4$, which is easily seen to be $1+\sum_{i<j} z_iz_j - (z_1z_2z_3+z_1z_2z_4+z_1z_3z_4+z_2z_3z_4)$. So $A = \varphi_t(\beta) = \frac{21}{16}$ and the C of Theorem 7.5′ is $\frac{1}{122}\frac{21}{16}$. Now $e_n = 256g(p^n\beta)$; by Theorem 7.5′ this is $\frac{168}{61}5^{3n} + \Delta_n$ where $\Delta_{n+1} = 3\Delta_n$. Since $e_0 = 1$, $\Delta_0 = -\frac{107}{61}$ and $\Delta_n = -\frac{107}{61}3^n$ for all n.

Example 3. We now calculate $e_n = e_n(2,2,2,2,2\,;3)$.

If $\beta = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$, then $3\beta = (1,1,1,1,1) + \beta$ and $9\beta = (4,4,4,4,4) + \beta$. So we are in the situation of Definition 7.6 with $\lambda = 2$, $u = 0$ and $t^{\#} = t = (4,4,4,4,4)$. Since $t^{\#} = 3(1,1,1,1,1) + (1,1,1,1,1)$, $l^{\#} = l_{t^{\#}} = l_{(1,1,1,1,1)} l_{(2-1,1,1,1,1)} = l^2_{(1,1,1,1,1)}$ and $\varphi_t(z) = l_{(1,1,1,1,1)} \varphi_{(1,1,1,1,1)}(1 - z_1, z_2, z_3, z_4, z_5) + 3^4 \varphi_{(1,1,1,1,1)} \left(\frac{(1,1,1,1,1)+z}{3}\right)$.

Therefore we need to calculate $l_{(1,1,1,1,1)}$ and $\varphi_{(1,1,1,1,1)}$. First we note that $D_F(2,1,1,1,1) = 1$, $D_F(2,2,1,1,1) = 2$, $D_F(2,2,2,1,1) = 3$, $D_F(2,2,2,2,1) = 6$ and $D_F(2,2,2,2,2) = 11$ (use Theorem 3.8). So $l_{(1,1,1,1,1)} = \sum_{\epsilon \in \{0,1\}^5} (-1)^{\Sigma \epsilon_i} D_F\big((1,1,1,1,1) + \epsilon\big) = 1 - \binom{5}{1} D_F(2,1,1,1,1) + \binom{5}{2} D_F(2,2,1,1,1) - \binom{5}{3} D_F(2,2,2,1,1) + \binom{5}{4} D_F(2,2,2,2,1) - D_F(2,2,2,2,2) = 1 - 5 \cdot 1 + 10 \cdot 2 - 10 \cdot 3 + 5 \cdot 6 - 11 = 5$ and $\varphi_{(1,1,1,1,1)}(z) = \sum_{\epsilon \in \{0,1\}^5} \left(\prod_{\epsilon_i = 1} z_i\right) \left(\prod_{\epsilon_i = 0} (1 - z_i)\right) D_F\big((1,1,1,1,1) + \epsilon\big) - 5(1 - z_1) z_2 z_3 z_4 z_5 = 1 + S_2 - S_3 + 3S_4 - 5S_5 - 5(1 - z_1) z_2 z_3 z_4 z_5 = 1 + S_2 - S_3 + 3S_4 - 5 z_2 z_3 z_4 z_5$ where S_j is the j^{th} symmetric function in $z_1, \ldots, z_5$. Therefore $l^{\#} = 5^2$ and, since $u = 0$, $A = \varphi_t(\beta) = 5\varphi_{(1,1,1,1,1)}(\beta) + 3^4 \varphi_{(1,1,1,1,1)}(\beta) = 86\left(1 + 10 \cdot (\frac{1}{2})^2 - 10 \cdot (\frac{1}{2})^3 + 3 \cdot 5 \cdot (\frac{1}{2})^4 - 5 \cdot (\frac{1}{2})^4\right) = 86 \cdot \frac{23}{8} = \frac{43 \cdot 23}{4}$. So the C of Theorem 7.5$'$ is $\frac{\frac{43 \cdot 23}{4}}{3^8 - 5^2} = \frac{23}{608}$.

Now $e_n = 32 g(p^n \beta)$; by Theorem 7.5$'$ this is $\frac{23}{19} 3^{4n} + \Delta_n$ with $\Delta_{n+2} = 25 \Delta_n$ for all n. Since $e_0 = 1$, $\Delta_0 = -\frac{4}{19}$. Furthermore $g\big((1,1,1,1,1) + z\big) = \varphi_{(1,1,1,1,1)}(z) + 5(1 - z_1) z_2 z_3 z_4 z_5$. So $g(3\beta) = g\big((1,1,1,1,1) + \beta\big) = \frac{23}{8} + \frac{5}{32} = \frac{97}{32}$, and $e_1 = 97$. We conclude that $\Delta_1 = \frac{23}{19} \cdot 81 - 97 = -\frac{20}{19}$, and that $\Delta_n = -\frac{4}{19} \cdot 5^n$ for all n.

References

1. P. Monsky : The Hilbert - Kunz Function, Math. Ann. **263**, 43-49 (1983)

2. P. Monsky : p - Ranks of Class Groups in $\mathbf{Z}_p^d$ - Extensions, Math. Ann. **263**, 509-514 (1983)

Appendix (Paul Monsky)

$l_F(k_1, \ldots, k_s)$ is p - multiplicative

Let F be a field. By an F - object we mean a finitely generated $F[T]$ - module on which T acts nilpotently. If M and N are F - objects so is $M \oplus N$. Furthermore $M \otimes_F N$ can be given the structure of F - object with $T(m \otimes n) = (T(m) \otimes n) + (m \otimes T(n))$. We will denote this F - object by $M \otimes N$.

Consider all formal differences $M - M'$ where M and M' are F - objects. We say that $M - M'$ and $N - N'$ are equivalent if $M \oplus N'$ and $M' \oplus N$ are isomorphic $F[T]$ - modules. The theory of Jordan canonical form (or the Krull - Schmidt theorem) shows that this is an equivalence relation. We denote the set of all equivalence classes of formal differences $M - M'$ by Γ. The following is easily proved :

Theorem A.1. *$\oplus$ and $\otimes$ induce binary operations, $+$ and $\cdot$, $\Gamma \times \Gamma \to \Gamma$. Under these operations Γ is a commutative ring and the unity element of Γ is the class of $F[T]/T$.*

Definition A.2. *If j is an integer ≥ 0, $[j] \in \Gamma$ is the class of $F[T]/T^j$, and $L_j = (-1)^j([j+1] - [j])$.*

Lemma A.3. *Γ is a free abelian group with the L_j forming a basis.*

Proof. The theory of Jordan canonical form shows that $[1], [2], [3], \ldots$ form a Z - basis of Γ. Since $[0]$ is the zero element of Γ, the result follows. ∎

Definition A.4. *$\alpha : \Gamma \to \mathbf{Z}$ is the Z - linear map $\sum c_i L_i \mapsto c_0$.*

Remark. α takes $[n]$ to 1 if $n > 0$. Suppose that V is an F - object. Writing V as a direct sum of copies of $F[T]/T^{n_j}$, $n_j > 0$, we see that $\alpha(V)$ is the number of summands. In other words $\alpha(V)$ is the F - dimension of V/TV. ∎

Theorem A.5. *Let $k_1, \ldots, k_s$ be non-negative integers. Then :*
(1) $\alpha(\prod_1^s [k_i]) = D_F(k_1, \ldots, k_s)$
(2) $\alpha(\prod_1^s L_{k_i}) = l_F(k_1, \ldots, k_s)$

Proof. Let $M_i = F[x_i]/x_i^{k_i}$ with T acting by multiplication by x_i. Each M_i is an F - object and $M_1 \otimes \cdots \otimes M_s$ identifies with $F[x_1, \ldots, x_s]/(x_1^{k_1}, \ldots, x_s^{k_s})$ with

T acting by multiplication by $\sum x_i$. (1) now follows from the definition of D_F and the remark after Definition A.4, and (1) together with Proposition 4.3 gives (2). ∎

Theorem A.6.
(1) $\alpha(L_iL_j) = \delta_{i,j}$
(2) $L_iL_j = \sum_k l_F(i,j,k)L_k$

Proof. Since $l_F(i,j) = \delta_{i,j}$, Theorem A.5 gives (1). We can write $L_iL_j = \sum_r c_{i,j,r}L_r$ with $c_{i,j,r} \in \mathbf{Z}$. Multiplying by L_k, applying α and using (1) together with Theorem A.5 we find that $c_{i,j,k} = l_F(i,j,k)$. ∎

Corollary A.7. $l_F(k_1,\ldots,k_s) \geq 0$.

Proof. Theorems 5.7, 5.9 and 5.21 show that $l_F(i,j,k)$ is either 0 or 1. In particular L_iL_j is a $\mathbf{Z}$ - linear combination of L_n with non-negative coefficients. It follows that $\prod_1^s L_{k_i}$ is a $\mathbf{Z}$ - linear combination of L_n with non-negative coefficients. But $l_F(k_1,\ldots,k_s) = \alpha\left(\prod L_{k_i}\right)$, the coefficient of L_0 in $\prod_1^s L_{k_i}$. ∎

From now on we assume char$F = p > 0$. We shall make extensive use of Theorem 5.21 which asserts that $l_F(k_1,k_2,k_3)$ is p - multiplicative.

Lemma A.8. *If* $k < p$, $L_{rp+k} = L_{rp} \cdot L_k$.

Proof. $L_{rp} \cdot L_k = \sum_t \sum_{j<p} l_F(rp,k,tp+j) \cdot L_{tp+j}$. Now if $r \equiv t \pmod 2$, $l_F(rp,k,tp+j) = l_F(r,t) \cdot l_F(k,j) = \delta_{r,t} \cdot \delta_{k,j}$, while if $r \not\equiv t \pmod 2$, $l_F(r,t) = 0$ and consequently $l_F(rp,k,tp+j) = 0$. ∎

Lemma A.9. *If* $(k_1,\ldots,k_s) \in I_p^s$, *then* $\prod_1^s L_{k_i}$ *is a* $\mathbf{Z}$ *- linear combination of* $L_0,\ldots,L_{p-1}$.

Proof. Suppose $r \geq p$. By Proposition 1.6, $D_F(k_1+\epsilon_1,\ldots,k_s+\epsilon_s,r+\epsilon_{s+1}) = \prod_1^s(k_i+\epsilon_i)$. Since the coefficient of $\epsilon_1\cdots\epsilon_{s+1}$ in this expression is zero, $l_F(k_1,\ldots,k_s,r) = 0$. So the coefficient of L_r in $\prod_1^s L_{k_i}$ is zero. (See the proof of Theorem A.6.) ∎

Lemma A.10. $L_{rp} \cdot L_{sp}$ *and* $L_{rp} \cdot L_{sp-1}$ *are* $\mathbf{Z}$ *- linear combinations of* L_{np} *and* L_{np-1} *with* $n \equiv r+s \pmod 2$.

Proof. Suppose that $j < p$ and the coefficient of L_{tp+j} in $L_{rp} \cdot L_{sp}$ is $\neq 0$. Then $l_F(rp,sp,tp+j) \neq 0$. But $l_F(rp,sp,tp+j) = l_F(r,s,t) \cdot l_F(0,j)$ or $l_F(r,s,t) \cdot l_F(0,p-1-j)$ according as $r+s+t$ is even or odd. So either $t \equiv r+s \pmod 2$, $j = 0$ and $tp+j = tp$, or $t-1 \equiv r+s \pmod 2$, $j = p-1$ and $tp+j = (t-1)p-1$. The argument for $L_{rp} \cdot L_{sp-1}$ is similar. ∎

Lemma A.11. *$\prod_1^s L_{r_i p}$ is a $\mathbf{Z}$ - linear combination of L_{np} and L_{np-1} with $n \equiv \sum r_i \pmod 2$.*

Proof. Lemma A.10 and induction. ∎

Lemma A.12. *There is an endomorphism ψ of Γ with the following properties :*
(1) $\psi(L_{rp}) = (-1)^{(p-1)r} L_r$ for all r
(2) If $u = \sum c_j L_j$, $\alpha\psi(u) = \sum_0^{p-1} (-1)^j c_j$

Proof. Suppose M is an F - object with $T_M : M \to M$ the multiplication by T map. Let $\psi(M)$ be the F - object which is M as vector space over F but with T operating by T_M^p. There is an obvious $\mathbf{Z}$ - linear map $\Gamma \to \Gamma$ taking the class of M to the class of $\psi(M)$ for all M ; we also denote this map by ψ. If M and N are F - objects, $\big((T_M \otimes 1) + (1 \otimes T_N)\big)^p = \sum_{i=0}^p \binom{p}{i} (T_M^p \otimes T_N^{p-i})$. Since F has characteristic p, this is $(T_M^p \otimes 1) + (1 \otimes T_N^p)$. So $\psi(M \otimes N)$ identifies with $\psi(M) \otimes \psi(N)$ as $F[T]$ - module and ψ is a ring endomorphism of Γ. If $k \leq p$ we see easily that $\psi([rp+k]) = (p-k)[r] + k[r+1]$. So if $k < p$, $\psi(L_{rp+k}) = (-1)^{rp+k}(-1)^r L_r$ giving (1) and (2). ∎

Lemma A.13. *Suppose $\prod_1^s L_{r_i p} = \sum c_j L_j$. Then :*
(1) If $\sum r_i$ is even, $c_0 = l_F(r_1, \ldots, r_s)$ and $c_1 = \cdots = c_{p-1} = 0$.
(2) If $\sum r_i$ is odd, $c_{p-1} = l_F(r_1, \ldots, r_s)$ and $c_0 = \cdots = c_{p-2} = 0$.

Proof. Lemma A.11 shows that $c_1 = \cdots = c_{p-1} = 0$ in case (1) and that $c_0 = \cdots = c_{p-2} = 0$ in case (2). Suppose we are in case (1). Then $\psi(\prod L_{r_i p}) = \prod \psi(L_{r_i p}) = \prod L_{r_i}$. So $\alpha\psi(\prod L_{r_i p}) = l_F(r_1, \ldots, r_s)$. On the other hand $\alpha\psi(\sum c_j L_j) = \sum_0^{p-1} (-1)^j c_j = c_0$. If we are in case (2), $\prod \psi(L_{r_i p}) = (-1)^{p-1} \prod L_{r_i}$. So $\alpha\psi(\prod L_{r_i p}) = (-1)^{p-1} l_F(r_1, \ldots, r_s)$ while $\alpha\psi(\sum c_j L_j) = (-1)^{p-1} c_{p-1}$ and $c_{p-1} = l_F(r_1, \ldots, r_s)$. ∎

Theorem A.14. *l_F is p - multiplicative for all s.*

Proof. Suppose $r \in I_\infty^s$ and $k \in I_p^s$. Then $l_F(rp+k) = \alpha\,(\prod_1^s L_{r_i p + k_i})$. By Lemma A.8 this is $\alpha\big((\prod_1^s L_{r_i p})(\prod_1^s L_{k_i})\big)$. Now write $\prod_1^s L_{r_i p} = \sum c_j L_j$. Since $\prod_1^s L_{k_i} = \sum_{j=0}^{p-1} l_F(j, k_1, \ldots, k_s) L_j$ (see Lemma A.9), Theorem A.6 (1) tells us that $l_F(rp+k) = \sum_0^{p-1} l_F(j, k_1, \ldots, k_s) c_j$. If r is even, apply Lemma A.13 (1). If r is odd, apply Lemma A.13 (2), and note that $l_F(p-1, k_1, \ldots, k_s) = l_F(p-1-k_1, k_2, \ldots, k_s)$ by Proposition 4.6. ∎