Local Galois Module Structure in Characteristic p.

Submitted by

Maria Louise Marklove

to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics, December 2013.

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other University.

. . . .

Maria Louise Marklove

Abstract

For a finite, totally ramified Galois extension L/K (of prime degree p) of local fields of characterstic p, we investigate the embedding dimension of the associated order, and the minimal number of generators over the associated order, for an arbitrary fractional ideal in L. This is intricately linked to the continued fraction expansion of $\frac{s}{p}$, where s is the ramification number of the extension. This investigation can be thought of as a generalisation of *Local Module Structure in Positive Characteristic* (de Smit & Thomas, Arch. Math 2007) - which was concerned with the rings of integers only - and also as a specific, worked example of the more general *Scaffolds and Generalized Integral Galois Module Structure* (Byott & Elder, arXiv:1308.2088[math.NT], 2013) - which deals with degree p^k extensions, for some k, which admit a Galois scaffold. We also obtain necessary and sufficient conditions for the freeness of these ideals over their associated orders. We show these conditions agree with the analogous conditions in the characteristic 0 case, as described in *Sur les idéaux d'une extension cyclique de degré premier d'un corps local* (Ferton, C.R. Acad. Sc. Paris, 1973).

Acknowledgements

As always, there are too many people and influences to mention, but here is an attempt. First and foremost, I thank Dr. Nigel Byott for his patience and guidance over the past three years, and my family for their continual encouragement, support and unwavering belief, irrespective of my endeavour. Gratitude also needs to be expressed to Alex Pettitt, Emily Drabek, Paul Williams, Alex Taylor, Iva Kavcic, Tim Paulden and Tim Jewitt - for their philosophical insights, advice, humour and friendship; to Linda McMillan, for sharing her mathematical enthusiasm all those years ago; and to Dee Bowker, for reigniting my creativity. Finally, to Ali Hunter, Ben Youngman, Dave Long, Lester Kwiatkowski, Robin Williams, and Theo Economou, for maintaining the concurrence of my sanity and insanity in the ebullient H319. I wish you all the best for the future.

Contents

Chapter 1

Introduction

The theory of Galois modules originally sought to investigate classical questions of algebraic number theory. For instance, one can use Galois Module Theory to great effect in order to describe the algebraic integers in a finite Galois extension of global or local fields. Let L/K be a finite Galois extension of number fields, with Galois group G, and let $\mathfrak{O}_K$ and $\mathfrak{O}_L$ be the rings of integers of the fields K and L respectively. The Normal Basis Theorem states that there exists an element $x \in L$ such that the set $\{\sigma(x) \mid \sigma \in G\}$ is a K-basis for L, i.e., L is a free module of rank 1 over the group algebra $K[G]$. It is an obvious extension, then, to consider the integral analogue of the Normal Basis Theorem, i.e., to ask when $\mathfrak{O}_L$ is free over the integral group ring $\mathfrak{O}_K[G]$. The freeness of $\mathfrak{O}_L$ is actually closely related to the ramification of the extension L/K. Recall L/K is said to be tame(ly ramified) if every prime ideal that ramifies has a ramification index prime to the characteristic of its residue field. Noether answered the question of local freeness with Theorem 1.1 (below), where we say $\mathfrak{O}_L$ is *locally free* over $\mathfrak{O}_K[G]$ if, for every prime $\mathfrak{p}$ of $\mathfrak{O}_K$, the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$ is a free module over the completed integral group ring, $\mathfrak{O}_{K,\mathfrak{p}}[G]$. Local freeness is a necessary, but not sufficient, condition for global freeness [Noe32][1].

Theorem 1.1. *(Noether's Criterion) Let L/K be a finite Galois extension of number fields with Galois group G, and $\mathfrak{O}_K \subset \mathfrak{O}_L$ the corresponding integer rings.*

[1] See also [Cha94] for a concise proof.

Then $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_K[G]$ if and only if L/K is tamely ramified.

When L/K is wildly ramified, then, Noether's Criterion tells us that $\mathfrak{O}_L$ is not locally free over $\mathfrak{O}_K[G]$. If we are to study wildly ramified extensions, we must therefore use another technique. One such technique is to enlarge the group ring $\mathfrak{O}_K[G]$ to a larger subring of the group algebra $K[G]$, namely the associated order:

Definition 1.2. *The* associated order *of $\mathfrak{O}_L$ is:*

$$\mathcal{A}_{L/K}(\mathfrak{O}_L) = \{\lambda \in K[G] : \lambda\mathfrak{O}_L \subset \mathfrak{O}_L\}$$

i.e., the set of all elements of $K[G]$ which induce endomorphisms on $\mathfrak{O}_L$.

The associated order is actually the largest $\mathfrak{O}_K$-order in $K[G]$ for which $\mathfrak{O}_L$ is a module. If L/K is at most tamely ramified then $\mathcal{A}_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K[G]$, but if the extension is wild then $\mathfrak{O}_K[G]$ is properly contained inside $\mathcal{A}_{L/K}(\mathfrak{O}_L)$.

In 1972 Marie-Josée Ferton gave necessary and sufficient conditions for the freeness of ideals of a local field, L (which we shall denote $\mathfrak{P}_L^h$ for some $h \in \mathbb{Z}$) in $\mathrm{char}(K) = 0$ [BF72]. In 2007, Bart de Smit and Lara Thomas explored the structure of $\mathfrak{O}_L$ - giving the minimal number of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$-generators and the embedding dimension of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ in $\mathrm{char}(K) = p$ [dST07]. The main topic of this thesis, then, is to utilise the methods of [dST07] to explore the structure of the $\mathfrak{P}_L^h$ over their associated orders in $\mathrm{char}(K) = p$. We give the minimal number of $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$-generators and the embedding dimension of $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ under certain, restricted cases, while finding necessary and sufficient conditions for freeness over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ similar to those stated in [BF72].

In Chapter 2 we cover some background information, including previous results on local fields in characteristic 0 and characteristic p, and remind ourselves of the Euclidean Algorithm and its relation to continued fractions.

In Chapter 3 we generalise the sets D (the size of which corresponds to the minimal number of associated order generators for $\mathfrak{O}_L$) and E (the size of which corresponds to the embedding dimension of the associated order $\mathfrak{O}_L$), as outlined in [dST07], in order to describe the generators and embedding dimension of $\mathfrak{P}_L$ (a prime ideal in L) and $\mathfrak{P}_L^h$ for some $h \in \mathbb{Z}$. We then compare this new definition of D and E to the sets in [BE13a] (which we call $\mathcal{D}$ and $\mathcal{E}$) and discover they are equivalent.

Chapter 4 formulates a pattern of residues, which we term *words*, and describes the general pattern for the case $h = s$, where s is the residue modulo p of the ramification number of the extension. We then invoke the use of a co-ordinate system in order to describe the pattern of residues when $h \neq s$.

In Chapter 5 we investigate the sets $\mathcal{D}$ and $\mathcal{E}$ further in order to obtain the main result of this thesis: given n (the length of the continued fraction expansion $\frac{s}{p} = [0; q_1, \ldots, q_n]$), we obtain the size and shape of $\mathcal{D}$ and $\mathcal{E}$ under certain restrictions relating to the value of h.

In Chapter 6, we remove the restrictions we enforced in Chapter 5 in order to obtain the general form of $\mathcal{D}$ and $\mathcal{E}$ when $n = 1$, $n = 2$, and $n = 3$. We also conjecture further descriptions of the sets $\mathcal{D}$ and $\mathcal{E}$ for general n.

In Chapter 7 we obtain corollaries to our main results. For instance, the analogous result (in $\mathrm{char}(K) = p$) of [Fer73] is a corollary to one of our theorems.

Chapter 2

Background

In this chapter we present the relevant background information, looking at known results for extensions of local fields of degree p^k, dealing with equal and unequal characteristic separately.

Before discussing the research literature, we recall the following definition, which may be found in any standard textbook on the subject (for example see [CF67], or [FT91]). Let L/K be a finite Galois extension of number fields with Galois group G, integer rings $\mathfrak{O}_L$ and $\mathfrak{O}_K$ (of L and K respectively), and ramification index $e = e(L/K)$ at $\mathfrak{P}_K$, a prime ideal of $\mathfrak{O}_K$. If $\mathfrak{P}_K$ has residue characteristic p, then we may define the following:

Definition 2.1. *We say L/K is:*

- *unramified at $\mathfrak{P}_K$ if $e = 1$;*
- *tamely ramified at $\mathfrak{P}_K$ if $p \nmid e$;*
- *wildly ramified at $\mathfrak{P}_K$ if $p | e$; and*
- *totally ramified at $\mathfrak{P}_K$ if $e = [L : K]$.*

As we mentioned in the Introduction, Noether's Theorem motivates us to study wildly ramified extensions of number fields, replacing $\mathfrak{O}_K[G]$ with $\mathcal{A}_{L/K}(\mathfrak{O}_L)$.

2.1 Wildly Ramified Extensions of Number Fields

In 1959, Leopoldt proved that for any abelian extension $L/\mathbb{Q}$, the ring $\mathfrak{O}_L$ is free over its associated order [Leo59]. Motivated by Noether's theorem, and the fact that the local context simplifies the problem dramatically, mathematicians over the past few decades have considered Galois module structures of rings of integers, for extensions of local fields.

2.1.1 Local Setup

A local field is a field K which is complete with respect to a discrete, surjective valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$. Let K be a local field of residue characteristic $p > 0$. Let L be a totally ramified Galois extension of K with cyclic Galois group, $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$. We define the ring of integers of K and L, respectively, as:

$$\mathfrak{O}_K = \{x \in K : v_K(x) \geq 0\} \quad \text{and} \quad \mathfrak{O}_L = \{x \in L : v_L(x) \geq 0\};$$

the unique maximal ideal of $\mathfrak{O}_K$ and $\mathfrak{O}_L$ respectively as:

$$\mathfrak{P}_K = \{x \in K : v_K(x) > 0\} \quad \text{and} \quad \mathfrak{P}_L = \{x \in K : v_L(x) > 0\};$$

and the residue field as:

$$\mathfrak{k} := \mathfrak{O}_K/\mathfrak{P}_K = \mathfrak{O}_L/\mathfrak{P}_L.$$

We assume k is perfect. When k has characteristic p, we have two cases:

1. Unequal characteristic - K has characteristic 0 and is therefore an extension of the field of p-adic numbers, $\mathbb{Q}_p$.

2. Equal characteristic - K also has characteristic p, and it can be identified with the field of formal power series, $k((\pi))$ for some uniformising element $\pi \in K$, i.e. $v_K(\pi) = 1$.

$\mathfrak{O}_L$ is an $\mathfrak{O}_K[G]$-module, and we are concerned with the freeness of $\mathfrak{O}_L$. (Note that in the local field case, $\mathfrak{O}_L$ is always free over $\mathfrak{O}_K$ since it is finite over a principal ring.) Before we begin the discussion of the two cases in more detail, we introduce one final, important concept.

Definition 2.2. *Let L/K be a finite Galois extension with Galois group G. The* ramification groups G_i *for $i \in \mathbb{Z}$, $i \geq -1$, of L/K are:*

$$G_i := \{\sigma \in G : v(\sigma(x) - x) \geq i + 1 \ \forall x \in \mathfrak{O}_L\}$$

or, equivalently:

$$G_i := \{\sigma \in G : \sigma(x) - x \in \mathfrak{P}_L^{i+1} \quad \forall x \in \mathfrak{O}_L\}.$$

These ramification groups form a decreasing filtration of normal subgroups of G [Ser68]:

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m \neq G_{m+1} = 1$$

for some integer $m \geq -1$. We also define the *ramification numbers* as the integers $b \geq -1$ such that $G_b \neq G_{b+1}$, i.e., where a *jump* occurs. These ramification numbers form an increasing sequence $b_1 < \ldots < b_r$, where $b_r = m$.

With these definitions, we can now also give an equivalent definition to Definition 2.1:

Definition 2.3. *L/K is:*

- *unramified if $G_0 = 1$;*
- *tamely ramified if $G_1 = 1$; and*
- *totally ramified if $G_0 = G$.*

It is worth noting that when K has prime residue characteristic p and L/K is a totally ramified p-extension (so $b_1 \geq 1$), then all the ramification numbers are congruent modulo p, i.e., $b_i \equiv b_j \pmod{p}$ for all i, j ([Ser68] IV §2, Proposition 11).

We will now separately deal with the equal and unequal characteristic cases of a local field K, surveying many of the existing results and indicating how we hope to extend some of these in the equal characteristic case.

2.1.2 Unequal Characteristic

Let K be local field with $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p$, where p is a fixed prime number. In this case, we may construct *Kummer extensions* in the following way: suppose K contains a primitive k-th root of unity, ζ_k. Pick $a \in K^\times$ such that $[a] \in K^\times/(K^\times)^k$ has order k. Then $L = K(\sqrt[k]{a})$ is a cyclic Kummer extension of K with

$$Gal(L/K) = C_k = \langle \sigma \rangle,$$

and $\sigma(\sqrt[k]{a}) = \zeta_k \sqrt[k]{a}$. In this case, the ramification jumps are bounded. In fact, as discussed in [Miy98], when k is a power of p, we have $b_r \leq \frac{e_K[L:K]}{p-1}$, where $e_K = v_K(p)$ is the absolute ramification index of K. Thus we have $b_r - \left\lfloor \frac{b_r}{p} \right\rfloor \leq p^{k-1}e_K$. Indeed, if $b_r < \frac{p^k e_K}{p-1}$ then $p \nmid b_i$ for all i, and if $b_r = \frac{p^k e_K}{p-1}$ then $p \mid b_i$ for all i.

We suppose that K is a finite extension of $\mathbb{Q}_p$. Leopoldt's Theorem is still true in this case, that is: for extensions of p-adic fields, $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ whenever $K = \mathbb{Q}_p$ and G is abelian. Byott showed that if L/K is an abelian extension of p-adic fields then $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ whenever L/K is at most weakly ramified, i.e., whenever its second ramification group is trivial [Byo99].

There are several known results for cyclic extensions L/K of degree p^k, for K a p-adic field. For the case $k = 1$, our problem was solved in its entirety in the 1970s by Bergé, Bertrandias (F. and J.P.) and Ferton. Bergé [Ber73], along with Bertrandias & Ferton [BF72] independently obtained the following result:

Theorem 2.4. *Let K be a p-adic field with uniformising element π. Let L/K be a totally ramified extension of degree p with ramification index e_K. Let $b < \frac{e_K p}{p-1} - 1$ be its unique ramification number, and σ a generator of its Galois group G. Let $f = \sigma - 1$. Then $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ is the $\mathfrak{O}_K$-submodule of $K[G]$ generated by the elements*

$$\frac{f^i}{\pi^{n_i}} \text{ for } i = 0, \ldots, p-1, \text{ where } n_i = \left\lfloor \frac{ib + \rho_i}{p} \right\rfloor,$$

and where $\rho_i = inf_{i \leq j \leq p-1} r_j$, with r_j the least non-negative residue of $-jb \pmod{p}$.

Clearly this theorem gives us an explicit description of $\mathcal{A}_{L/K}$ in the case of totally ramified, cyclic extensions of degree p. F. Bertrandias, J-P. Bertrandias and Ferton then went on to give necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over its associated order [BBF72]:

Theorem 2.5. *Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified extension of degree p with ramification number b and ramification index $e_K = e(L/K)$.*

1. *If $p \mid b$, then $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$.*
2. *If $p \nmid b$ then let $b = q_0p + s$, where $1 \leq s \leq p-1$. In this case:*
   - *if $1 \leq b < \frac{pe_K}{p-1} - 1$, then $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $s \mid p-1$;*
   - *if we let $\frac{b}{p} = [q_0; q_1, \ldots, q_n]$, $q_n \geq 2$ be shorthand for the continued fraction expansion:*

$$\frac{b}{p} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots \, \cfrac{}{q_{n-1} + \frac{1}{q_n}}}},$$

then if $b \geq \frac{pe_K}{p-1} - 1$, $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $n \leq 4$.

There is much less known for cyclic extensions in the general case, i.e., when L/K has degree p^k for $k > 1$. Some works of note towards this include that of Miyata [Miy98], who studied the conditions of Ferton and Bertrandias (as above) when L/K is totally ramified, for a certain cyclic Kummer extension of degree p^k. Later, Byott [Byo08] deduced from Miyata's result that $\mathfrak{O}_K$ is free over its associated order if $b \mid (p^m - 1)$, for some m with $1 \leq m \leq k$, where b is the least non-negative residue of $b_1 \pmod{p^k}$, the first ramification number of L/K. He also shows that the converse holds when $k = 2$. The proof requires some intricate combinatorial calculations, and Byott also introduces a somewhat complicated set, $S(p^k)$, showing that $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $b \in S(p^k)$.

Aside from the ring of integers, $\mathfrak{O}_L$, it is interesting to ask ourselves if a general ideal, $\mathfrak{P}_L^h$ (for some h) is free over its associated order,

$$\mathcal{A}_{L/K}(\mathfrak{P}_L^h) = \{\lambda \in K[G] : \lambda\mathfrak{P}_L^h \subset \mathfrak{P}_L^h\}.$$

In 1973, Ferton gave us the following result [Fer73]:

Theorem 2.6. *Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified, cyclic extension of degree p with ramification number $b = q_0 p + s$, and let $0 \leq h < p$.*

1. *If $b \equiv 0 \pmod{p}$, then $\mathfrak{P}^h$ is free over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ for all h.*

2. *If $b \equiv 1 \pmod{p}$ and if $1 \leq b < \frac{pe}{p-1} - 2$, then $\mathfrak{P}^h$ is free over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ if and only if $h = 0$, $h = 1$ or $h > \frac{p+1}{2}$.*

3. *If $b \not\equiv 0$, $b \not\equiv 1 \pmod{p}$, then:*

   (a) if $1 \leq b < \frac{pe}{p-1} - 2$ and h satisfies $s < h \leq p-1$, then $\mathfrak{P}^h$ is not free over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$;

   (b) if $1 \leq b < \frac{pe}{p-1} - 1$ and h satisfies $0 \leq h \leq s$, then $\mathfrak{P}^h$ is free over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ if and only if the following conditions are satisfied: let $\frac{b}{p} = [q_0; q_1, \ldots, q_n]$, $q_n > 1$ be shorthand for the continued fraction expansion, as before. Then,

   - *for n even: $h = s$ or $h = s - q_n$;*
   - *for n odd: $s - \frac{1}{2}q_n \leq h \leq s$.*

Note the dependency on parity in this last case. This is due to the truncation of the continued fraction expansion at point n - which will give either an over- or an under-estimate of $\frac{s}{p}$. This means we have these slightly complicated conditions that, although they may not look particularly neat, give a very powerful result - we can now determine precisely when an ideal will or will not be free over its associated order. It is a reasonable question to ask if this theorem is also true in the $char(K) = p$ case. The answer turns out to be the affirmative, as we will see in Chapter 7.

2.1.3 Equal Characteristic

We now deal with the case when $\text{char}(K) = \text{char}(k) = p$ and L/K has order p^k. In this case, we can use Artin-Schreier Theory to construct extensions in the following way: take $a \in K$ such that $x^p - x - a = 0$ is irreducible in K. Then if $L = K(x)$,

L/K is a Galois extension of degree p and:

$$(x+1)^p - (x+1) = x^p + 1 - (x+1) = a.$$

The roots of this equation are clearly $x, x+1, x+2, \ldots, x+(p-1)$. Hence our Galois group G is generated by σ where $\sigma(x) = x+1$. More generally, if $q = p^r$ and $\mathbb{F}_q \subseteq K$, take $x^q - x - a = 0$ for any a where this is irreducible. For $w \in \mathbb{F}_q$,

$$(x+w)^q - (x+w) = x^q - x + (w^q - w) \quad = x^q - x = a.$$

So now, if $L = K(x)$, then $G = Gal(L/K) \cong (\mathbb{F}_q)^+ \cong \underbrace{C_p \times \ldots \times C_p}_{r \text{ times}}$. If the residue field, $\mathfrak{k}$, is perfect, then all the ramification jumps are relatively prime to p. Importantly, we also have that the ramification jumps are not bounded as L varies.

In this equal characteristic case, the group algebra $K[G]$ is a local ring whose maximal ideal is the ideal generated by all $\sigma - 1$, where σ runs through the elements of G. The associated order is also a local ring.

Once again, when $k = 1$, our question for the valuation ring $\mathfrak{O}_L$ itself has been solved in its entirety. If L/K is a totally ramified extension of degree p then it has a unique ramification number which is prime to p, i.e., we can write $b = q_0 p + s$, where $1 \leq s \leq p-1$. In the equal characteristic case, we use Artin-Schreier Theory to find an $A \in K$ with $L = K(\alpha)$, where $\alpha^p - \alpha = A$ and $v_K(A) = -b$.

The work of Aiba [Aib03], which had a minor error later corrected by Lettl [Let05], can be restated as a result corresponding to [BBF72], but for characteristic p:

Theorem 2.7. *$\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $s|(p-1)$.*

This result was then later reinterpreted by Bart de Smit and Lara Thomas in a more algebraic way [dST07]: let

$$edim(\mathcal{A}_{L/K}) := dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2}$$

be the embedding dimension of $\mathcal{A}_{L/K}$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{A}_{L/K}$. Then $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if $edim(\mathcal{A}_{L/K}) \leq 3$. Later, in Chapter 6, we will show that this is not the case for $\mathfrak{P}_L^h$.

In a sense, this embedding dimension is a measure of the complexity of $\mathcal{A}_{L/K}$, while the minimal number of generators of $\mathfrak{O}_L$ over $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ (which, given the continued fraction expansion of p and s, de Smit and Thomas also computed; see Theorem 2.8) is a measure of the complexity of the structure of $\mathfrak{O}_L$.

Theorem 2.8. *Let K be a local field with char$(K) = p$, and let L/K be a totally ramified cyclic extension of degree p. Let $b = q_0 p + s$ be the unique ramification number of L/K, with $1 \leq s \leq p-1$. Let d be the minimal number of generators of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$. Then $d = 1$ if and only if $\mathfrak{O}_L$ is free over $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ and:*

1. *if $s = p-1$ then $d = 1$ and edim$(\mathcal{A}_{L/K}(\mathfrak{O}_L)) = 2$;*

2. *if $s < p-1$ then edim$(\mathcal{A}_{L/K}(\mathfrak{O}_L)) = 2d+1$ and $d = \sum_{i<n,\ i \text{ odd}} b_i$, where the b_i are the unique integers given by the continued fraction expansion:*

$$-\frac{s}{p} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots \cfrac{\ddots}{b_{n-1} + \frac{1}{b_n}}}}$$

   where $b_1, \ldots, b_n \geq 1$ and $b_n \geq 2$.

In particular, $\mathfrak{O}_L$ is free over its associated order if and only if $s \mid (p-1)$. In each case, we can explicitly find a set of $\mathfrak{O}_K$-generators of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ and a minimal set of generators of $\mathfrak{O}_L$ over $\mathcal{A}_{L/K}(\mathfrak{O}_L)$.

Remark 2.9. *This theorem uses the continued fraction expansion of $-\frac{s}{p}$, whereas Theorems 2.5 and 2.6 used the continued fraction expansion of $+\frac{b}{p}$. These are related quantities. Namely, if $\frac{b}{p} = [q_0; q_1, \ldots, q_n]$ then*

$$-\frac{s}{p} = \begin{cases} [-1; 1, q_1 - 1, q_2, \ldots, q_n] & \text{if } q_1 > 1 \\ [-1; q_2 + 1, q_3, \ldots, q_n] & \text{if } q_1 = 1. \end{cases}$$

To see this, first look at the case when $q_1 > 1$. *Let* $\alpha = [0; q_2, \ldots, q_n]$. *Then*

$$
\begin{aligned}
[-1; 1, q_1 - 1, q_2, \ldots, q_n] &= -1 + \cfrac{1}{1 + \frac{1}{q_1 - 1 + \alpha}} \\
&= -1 + \frac{q_1 - 1 + \alpha}{q_1 + \alpha} \\
&= -1 + 1 - \frac{1}{q_1 + \alpha} \\
&= -\frac{1}{q_1 + \alpha} \\
&= -[0; q_1, \ldots, q_n].
\end{aligned}
$$

Now look at the case when $q_1 = 1$. *Given* $[0; q_1, \ldots, q_n]$, *write:*

$$
\begin{aligned}
&1 = q_1 \\
&q'_1 - 1 = q_2 \\
&q'_2 = q_3 \\
&\vdots \\
&q'_{n-1} = q_n.
\end{aligned}
$$

Then $[0; q_1, \ldots, q_n] = [-1; 1, q'_1 - 1, q'_2, \ldots, q'_{n-1}] = -[0, q'_1, \ldots, q'_{n-1}]$.

The proof of Theorem 2.8 is very clever, and uses a mixture of combinatorics with balanced sequences and graded rings. Namely, the associated order is given the structure of a graded ring, while $\mathfrak{O}_L$ is given the structure of a graded module over it. In Chapter 3 of this thesis, we prove another result using this method, but for $\mathfrak{P}_L^h$ instead. It is also possible that perhaps a similar method can be used when considering cyclic extensions of degree p^k, for some $k \geq 2$, in this $char(K) = p$ case.

In the case where G is no longer necessarily cyclic but is elementary abelian, Byott and Elder have investigated a family of abelian extensions [BE13b], obtaining a criterion which interestingly agrees with previous work by Miyata (for Kummer extensions of characteristic 0, [Miy98]). For k a perfect field of characteristic p, and $K = k((T))$, Byott and Elder obtain a necessary and sufficient condition for $\mathfrak{O}_L$ to be free over $\mathcal{A}_{L/K}$ for large classes of extensions of equal characteristic. For this they have used the existence of a Galois Scaffold, as described in Elder's paper

[Eld09], which essentially is the existence of a valuation criterion and a certain *nice* basis. Moreover, Byott and Elder give an explicit basis for the associated order of $\mathfrak{O}_L$, as well as giving a generator of $\mathfrak{O}_L$ over its associated order when $\mathfrak{O}_L$ is free over it.

From here it is reasonable to ask if an analogue of Theorem 2.8 holds for a general ideal, $\mathfrak{P}_L^h$, as well as just $\mathfrak{O}_L$, at least for the case when the extension L/K has degree p. In this thesis, then, we consider and use the methods of [dST07] (which deals with the freeness of $\mathfrak{O}_L$ over its associated order in $\mathrm{char}(K) = p$) and apply them to see if the results of [BF72] (which obtains necessary and sufficient conditions for the freeness of $\mathfrak{P}_L^h$, for $h \in \mathbb{Z}$, over its associated order in $\mathrm{char}(K) = 0$) can be obtained for the freeness of $\mathfrak{P}_L^h$ over its associated order in $\mathrm{char}(K) = p$, for Galois extensions of degree p. Recent work by Huynh has also shown this [Huy14] - that the analogous results of [BF72] can be achieved in the $\mathrm{char}(K) = p$ case - using methods which differ to those seen in the following chapters.

We have now covered the main background relevant to this thesis, but for a full survey of results within the theory of Galois module structures for extensions of local fields, the author highly recommends [Tho10]. We shall now conclude this chapter with a review of the Euclidean Algorithm, as this will be useful to our discussion later.

2.2 The Euclidean Algorithm and Continued Fractions

Let s, p be integers with $0 < s < p$ and $\gcd(s, p) = 1$. (We don't require p to be prime for the moment.) We first make explicit how the two forms of the continued fraction expansion of $\frac{s}{p}$ are related to two versions of the Euclidean Algorithm. We begin both versions by setting $r_{-1} = p$, $r_0 = s$, $q_0 = 0$. For $j \geq 1$, define integers q_j, r_j by

$$r_{j-2} = q_j r_{j-1} + r_j, \qquad 0 \leq r_j < r_{j-1} \tag{2.1}$$

until we reach $r_m = \gcd(p, s) = 1$. In the first (standard) version, set $n = m + 1$ and carry on for one more step, so $q_n = q_{m+1} = r_{m-1} \geq 2$ and $r_n = r_{m+1} = 0$. In the second (non-standard) version, set $n = m + 2$, $q_{m+1} = r_{m-1} - 1$, $r_{m+1} = 1$ and $q_n = q_{m+2} = 1$, $r_n = r_{m+2} = 0$. Thus in both versions, the algorithm terminates with $r_n = 0$ (but for different values of n). The equality in (2.1) holds in all cases, but, in the second version of the algorithm, the condition $r_j < r_{j-1}$ fails for $j = n - 1$.

When we calculate the continued fraction expansion of $\frac{s}{p}$, we carry out the same sequence of divisions as for the Euclidean algorithm, so the partial quotients of the continued fraction are the q_j obtained above. The first version of the Euclidean algorithm gives the standard form of the continued fraction expansion:

$$\frac{s}{p} = [q_0; q_1, \ldots, q_n] = [0; q_1, \ldots, q_m, r_{m-1}] \text{ with } q_n \geq 2.$$

The second version gives the alternative, slightly longer, form

$$\frac{s}{p} = [q_0; q_1, \ldots, q_n] = [0; q_1, \ldots, q_m, r_{m-1} - 1, 1] \text{ with } q_n = 1.$$

In both versions of the Euclidean algorithm, let $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$, and define $x_j = q_{j-1}x_{j-1} + x_{j-2}$, $y_j = q_{j-1}y_{j-1} + y_{j-2}$ for $1 < j \leq n + 1$. In particular, $x_2 = 1$ and $y_2 = q_1$. Then we have the Bezout identity

$$x_j r_{-1} - y_j r_0 = x_j p - y_j s = (-1)^j r_{j-1};$$

this can be verified by induction, where the induction step uses the *two* preceding cases. In particular,

$$x_{n+1}p - y_{n+1}s = (-1)^{n+1} r_n = 0.$$

Lemma 2.10. *For either version of the Euclidean algorithm, we have*

$$x_{n+1} = s, \qquad y_{n+1} = p.$$

Proof. Let q'_j, r'_j, x'_j, y'_j be the values corresponding to q_j, r_j, x_j, y_j when we apply the same version of the Euclidean Algorithm to (r_1, s) in place of (s, p). Since this involves the same sequence of divisions as before (with the first omitted), we have $q'_j = q_{j+1}$, $r'_j = r_{j+1}$ for $1 \leq j \leq n$. We have $x_1 = 0 = y'_0$, $x_2 = 1 = y'_1$, $y_1 = 1 = x'_0 + q_1 y'_0$, $y_2 = q_1 = x'_1 + q_1 y'_1$. It then follows inductively that $x_{j+1} = y'_j$ and $y_{j+1} = x'_j + q_1 y'_j$ for $0 \leq j \leq n$, since each side of either equation satisfies the same degree 2 recurrence relation.

We now prove the lemma by induction. If $n = 1$ then $s = 1$, $q_1 = p$, $r_1 = 0$, so that $x_2 = px_1 + x_0 = x_0 = 1 = s$ and $y_2 = py_1 + y_0 = p$. Thus the Lemma holds when $n = 1$. Now let $n \geq 2$, and let x'_n, y'_n be obtained from the pair (r_1, s) as above. By the induction hypothesis we have $x'_n = r_1$ and $y'_n = s$, so that $x_{n+1} = y'_n = s$ and $y_{n+1} = x'_n + q_1 y'_n = r_1 + q_1 s = p$, as required. □

Corollary 2.11. *Let $\frac{s}{p} = [0; q_1, \ldots, q_n]$ be the standard continued fraction expansion of $\frac{s}{p}$. Then, for $1 \leq j \leq n$, the truncated expansion $[0; q_1, \ldots, q_j]$ (where possibly $q_j = 1$) evaluates to x_{j+1}/y_{j+1}.*

Proof. Let $[0, q_1, \ldots, q_j] = \frac{u}{v}$ in lowest terms. Apply the Euclidean Algorithm to the pair (u, v), using the first version if $q_j \geq 2$ and the second version if $q_j = 1$. Since the partial quotients for (u, v) are the same as those for (p, s) (but stopping at step j), we get the same values for the x_i and y_i, up to $i = j+1$. For the pair (u, v), Lemma 2.10 then gives $x_{j+1} = u$, $y_{y+1} = v$, so that $[0; q_1, \ldots, q_j] = x_{j+1}/y_{j+1}$. □

We are now in a position to begin discussing the [dST07] paper in more detail, which defines sets D and E in order to describe the minimal number of generators of $\mathfrak{O}_L$, and the embedding dimension of $\mathcal{A}_{L/K}(\mathfrak{O}_L)$ respectively, for degree p extensions of local fields in $\mathrm{char}(K) = p$.

Chapter 3

The Sets $\mathcal{D}$ and $\mathcal{E}$

Recall that we are concerned with degree p extensions L/K, with perfect residue field, and where $b = q_0 p + s$ is the ramification number. Take $\theta \in L$ with $v_L(\theta) = -(p-1)b$.

As in [dST07], we can choose a generator σ for $G = Gal(L/K)$, and write $X = \sigma - 1 \in K[G]$. Then $K[G]$ is the truncated polynomial ring $K[X]/(X^p)$, and $K[G]$ becomes a graded ring whose homogeneous part of degree i is non-trivial only if $i = 0, \ldots, p-1$, in which case it is the 1-dimensional K-vector space KX^i.

Since we are working in the case where $\mathrm{char}(K) = p$ then, as in [dST07], we may use Artin-Schreier theory. For $i < p$, the element $\binom{\alpha}{i}$ is the binomial polynomial

$$\binom{\alpha}{i} = \frac{\alpha(\alpha-1)\ldots(\alpha-i+1)}{i!},$$

where $\binom{\alpha}{0} = 1$ and $\binom{\alpha}{i} = 0$ for $i < 0$. So now take $\theta = \binom{\alpha}{p-1}$ where $L = K(\alpha)$ and $\alpha^p - \alpha = a \in K$, with $v_K(a) = -b \not\equiv 0 \pmod{p}$. We choose the generator σ of G so that $\sigma\alpha = \alpha + 1$. For $i < p$, we have $(\sigma - 1)\binom{\alpha}{i} = \binom{\alpha}{i-1}$. This means we can equip L with the structure of a graded module over $K[G]$, where its homogeneous piece of degree i is the one-dimensional K-vector space

$$L_i = K\binom{\alpha}{p-i} = K(\theta)$$

for $i = 1, \ldots, p$ (and $L_i = 0$ for $i = 0$ or $i > p$), while the homogeneous piece of degree j in $K[G]$ is $K(\sigma-1)^j$, for $0 \leq j \leq p-1$.

We are concerned with the structure of $\mathfrak{O}_L$ and $\mathfrak{P}^h := \mathfrak{P}^h_L$ (for some fixed $h \in \mathbb{Z}$) as $\mathcal{A}(\mathfrak{O}_L)$ and $\mathcal{A}(\mathfrak{P}^h)$ modules respectively. As in [dST07], we define the following for $j \in \mathbb{Z}$:

$$a_j = \lceil jx \rceil \quad \text{where } x = \frac{s}{p}, \text{ so } 0 < x < 1;$$

$$\varepsilon_j = a_j - a_{j-1};$$

$$m_j = \inf\{\varepsilon_{i+1} + \varepsilon_{i+2} + \ldots + \varepsilon_{i+j} : 0 \leq i \leq p - j - 1\}, \text{ for } j \geq 0,$$

or, equivalently, $m_j = \min_{0 \leq i < p-j} \{a_{i+j} - a_i\}$;

$$D = \{i : 0 < i < p \text{ and } a_j + m_{i-j} < a_i \text{ for all } j \text{ with } 0 < j < i\};$$

$$E = \{i : 0 \leq i < p \text{ and } m_j + m_{i-j} < m_i \text{ for all } j \text{ with } 0 < j < i\}.$$

Note that, as in [dST07], we always have $1 \in D$ and $0, 1 \in E$. Recall - as mentioned in the previous Chapter - that [dST07] defined the embedding dimension of $\mathcal{A}_{L/K}$ as

$$edim(\mathcal{A}_{L/K}) := dim_k \frac{\mathfrak{m}}{\mathfrak{m}^2},$$

where $\mathfrak{m}$ is the maximal ideal of $\mathcal{A}_{L/K}$. We may now state Theorem 4 of [dST07]:

Theorem 3.1. *The minimal number of $\mathcal{A}(\mathfrak{O}_L)$-module generators of $\mathfrak{O}_L$ is $|D|$ and* $\mathrm{edim}(\mathcal{A}(\mathfrak{O}_L)) = |E|$. *Moreover, a set of homogeneous elements in $\mathfrak{O}_L$ (respectively $\mathfrak{m}$) forms a set of $\mathcal{A}(\mathfrak{O}_L)$-module generators of $\mathfrak{O}_L$ (respectively $\mathfrak{m}$) if and only if for each $i \in D$ (respectively E) it contains an $\mathcal{A}(\mathfrak{O}_L)$-module generator of $(\mathfrak{O}_L)_i$ (respectively $\mathfrak{m}_i$).*

Our aim now is to give analogous definitions of these sets D and E, but for general $\mathfrak{P}^h$ (for some h).

For $i = 1, \ldots, p$, $\binom{\alpha}{p-i}$ has valuation $-(p-i)b \equiv ib \pmod{p}$. Let π be a uniformising element, i.e., $v_K(\pi) = 1$, and write $b = q_0 p + s$. Now define:

$$A_j^{(h)} = \left\lceil \frac{jb + h}{p} \right\rceil; \qquad a_j^{(h)} = \left\lceil \frac{js + h}{p} \right\rceil$$

so that

$$A_j^{(h)} = a_j^{(h)} + jq_0.$$

Also define

$$\varepsilon_j^{(h)} = a_j^{(h)} - a_{j-1}^{(h)};$$
$$m_n^{(h)} = \min\{\varepsilon_{i+1}^{(h)} + \ldots + \varepsilon_{i+n}^{(h)} : 0 \leq i \leq p-n-1\}, \text{ with } m_0 = 0;$$
$$D^{(h)} = \{i : 1 \leq i \leq p : a_{p-i}^{(h)} + m_{i-j}^{(h)} < a_{p-j}^{(h)} \text{ for all } j \text{ with } 1 \leq j < i\};$$
$$E^{(h)} = \{i : 0 \leq i < p : m_j^{(h)} + m_{i-j}^{(h)} < m_i^{(h)} \text{ for all } j \text{ with } 0 < j < i\}.$$

Notice that our definition of $D^{(h)}$ differs slightly from the set D of [dST07] as our numbering has been reversed. However, our form is the more general form of numbering; indeed, as discussed in the proof of Theorem 5 of [dST07], de Smit and Thomas are able to reverse their numbering when $h = 0$ since, in this case, $a_j + a_{p-j} = s$ for $1 \leq j \leq p-1$.

Theorem 3.2. *$|D^{(h)}|$ gives us the minimal number of $\mathcal{A}(\mathfrak{P}^h)$-module generators of $\mathfrak{P}^h$, and $|E^{(h)}| = \operatorname{edim}(\mathcal{A}(\mathfrak{P}^h))$.*

Proof. By generalising Proposition 3 of [dST07], we construct the following argument. Firstly, we claim the following: for π a uniformising element of $\mathfrak{O}_K$,

$$\pi^{A_{p-i}^{(h)}} \binom{\alpha}{p-i}$$

with $1 \leq i \leq p$, is an $\mathfrak{O}_K$-basis of $\mathfrak{P}^h$. We certainly have

$$\mathfrak{P}^h \supseteq \mathcal{M},$$

where $\mathcal{M}$ is the module

$$\mathcal{M} = \bigoplus_{i=1}^{p} \mathfrak{O}_K \pi^{A_{p-i}^{(h)}} \binom{\alpha}{p-i}.$$

Then

$$\mathcal{M} + \pi\mathfrak{P}^h = \mathfrak{P}^h.$$

Applying Nakayama's Lemma to $\mathfrak{O}_K$-modules we have

$$\mathcal{M} = \mathfrak{P}^h,$$

as required. So now define

$$(\mathfrak{P}^h)_i := \pi^{A_{p-i}^{(h)}} \mathfrak{O}_K \binom{\alpha}{p-i},$$

so $\mathfrak{P}^h = \bigoplus_{i=1}^{p} (\mathfrak{P}^h)_i$, and write $b = q_0 p + s$, for $0 \le s \le p-1$. Then we have:

$$(\mathfrak{P}^h)_i = \pi^{q_0(p-i)+a_{p-i}^{(h)}} \mathfrak{O}_K \binom{\alpha}{p-i}, \text{ where } a_{p-i}^{(h)} = \left\lceil \frac{(p-i)s+h}{p} \right\rceil,$$

as $A_{p-i}^{(h)} = (p-i)q_0 + a_{p-i}^{(h)}$. Now let $\phi = \frac{\sigma-1}{\pi^{q_0}} \in K[G]$. Then, since $(\sigma-1)\binom{\alpha}{p-i} = \binom{\alpha}{p-(i+1)}$ and

$$\pi^{-q_0} \mathfrak{P}^{A_{p-i}^{(h)}} \binom{\alpha}{p-i-1} = \pi^{\psi} \mathfrak{P}^{A_{p-1-i}^{(h)}} \binom{\alpha}{p-i-1},$$

where

$$\begin{aligned} \psi &= -q_0 p + A_{p-i}^{(h)} - A_{p-i-1}^{(h)} \\ &= -q_0 p + (p-i)q_0 + a_{p-i}^{(h)} - (p-i-1)q_0 - a_{p-i-1}^{(h)} \\ &= a_{p-i}^{(h)} - a_{p-i-1}^{(h)} \\ &= \varepsilon_{p-i}^{(h)}, \end{aligned}$$

we have

$$\phi(\mathfrak{P}^h)_i = \pi^{\psi} (\mathfrak{P}^h)_{i+1}.$$

Similarly, $\mathcal{A}(\mathfrak{P}^h) = \bigoplus_{i=0}^{p-1} \mathcal{A}(\mathfrak{P}^h)_i$, with

$$\begin{aligned} \mathcal{A}(\mathfrak{P}^h)_i &= \{\lambda \in K\phi^i : \lambda(\mathfrak{P}^h)_j \subset (\mathfrak{P}^h)_{j+i} \ \forall j : 1 \le j \le p-i\} \\ &= \mathfrak{P}^{-m_i^{(h)}} \phi^i, \end{aligned} \tag{3.1}$$

where $m_i^{(h)} = \min\{\varepsilon_{p-i-j+1}^{(h)} + \ldots + \varepsilon_{p-j}^{(h)} : 0 \le j \le p-i\}$.

Now we shall generalise Theorem 4 of [dST07]. For clarity, let $\mathfrak{p}$ be the unique maximal ideal of $\mathfrak{O}_K$. Recall that, for a fixed $h \in \mathbb{Z}$, $\mathfrak{m}$ is the maximal ideal of $\mathcal{A}(\mathfrak{P}^h)$, and $\mathfrak{m} = \bigoplus_{i=0}^{p-1} \mathfrak{m}_i$, with $\mathfrak{m}_0 = \mathfrak{p}$ and $\mathfrak{m}_i = \mathcal{A}(\mathfrak{P}^h)_i$, for $i > 0$. This implies $\mathfrak{m}\mathfrak{P}^h$ is a graded submodule of $\mathfrak{P}^h$. We have:

$$(\mathfrak{m}\mathfrak{P}^h)_i = \sum_{j=1}^{i-1} \mathfrak{m}_{i-j} (\mathfrak{P}^h)_j + \mathfrak{m}(\mathfrak{P}^h)_i.$$

Thus,

$$(\mathfrak{m}\mathfrak{P}^h)_i = (\mathfrak{P}^h)_i \ \Leftrightarrow \ a_{p-j}^{(h)} - m_{i-j}^{(h)} = a_{p-i}^{(h)} \text{ for some } j : 1 \le j < i.$$

Now take $i = p$, $j = 1$ and, without loss of generality, $0 \leq h < p$:

$$\begin{aligned} a_{p-1}^{(h)} - m_{p-1}^{(h)} &= a_{p-1}^{(h)} - (a_{p-1}^{(h)} - a_0^{(h)}) \\ &= a_0^{(h)} = \begin{cases} 0 \text{ if } h = 0 \\ 1 \text{ if } h > 0. \end{cases} \end{aligned}$$

Thus $(\mathfrak{m}\mathfrak{P}^h)_i = \mathfrak{P}_i^h \;\Leftrightarrow\; i \notin D^{(h)}$, where:

$$D^{(h)} = \{i : 1 \leq i \leq p : a_{p-i}^{(h)} + m_{i-j}^{(h)} < a_{p-j}^{(h)} \text{ for all } j \text{ with } 1 \leq j < i\}.$$

Similarly, we have:

$$(\mathfrak{m}^2)_i = \sum_{j=0}^{i} \mathfrak{m}_j \mathfrak{m}_{i-j}.$$

Thus,

$$\begin{aligned} (\mathfrak{m}^2)_i = (\mathfrak{m})_i \;&\Leftrightarrow\; m_i^{(h)} = m_j^{(h)} + m_{i-j}^{(h)} \text{ for some } j : 0 < j < i \\ &\Leftrightarrow i \notin E^{(h)}, \end{aligned}$$

where $E^{(h)} = \{i : 0 \leq i < p : m_j^{(h)} + m_{i-j}^{(h)} < m_i^{(h)} \text{ for all } j \text{ with } 0 < j < i\}$. □

We now turn to [BE13a] which considers the more general case of degree p^n extensions (for some n), in both characteristic p and characteristic 0, in which there exists a Galois Scaffold (of tolerance $l \geq p^n + b - h$, in the language of the authors). In the case that we are concerned with, i.e., degree p extensions in $\mathrm{char}(K) = p$, there always exists such a Galois Scaffold. We are therefore working in a special case of that discussed in [BE13a]. The authors define:

$$\mathbb{S}_{p^n} = \{0, 1, \ldots, p^n - 1\}, \qquad \mathbb{S}_p = \{0, 1, \ldots, p - 1\},$$

and identify each $x \in \mathbb{S}_{p^n}$ with its vector of base-p coefficients:

$$(x) = (x_{(n-1)}, \ldots, x_{(0)}) \in \mathbb{S}_p^n,$$

where $x = \sum_{i=0}^{n-1} x_{(i)} p^i$. They endow $\mathbb{S}_{p^n}$ with a partial order, writing $x \preceq y$ if and only if $x_{(i)} \leq y_{(i)}$ for all $0 \leq i \leq n-1$, and they let $r : \mathbb{Z} \to \mathbb{S}_{p^n}$ be the residue function $r(l) \equiv l \pmod{p^n}$. For integers $b_1, \ldots, b_n$ such that $p \nmid b_1, \ldots, b_n$, they then define a function $\mathfrak{b} : \mathbb{S}_{p^n} \to \mathbb{Z}$:

$$\mathfrak{b}(x) = \sum_{i=1}^{n} x_{(n-i)} p^{n-i} b_i.$$

The function $r \circ (-\mathfrak{b}) : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$ is defined by $r \circ (-\mathfrak{b})(x) = r(-\mathfrak{b}(x))$ and is a bijection, with its inverse denoted $\mathfrak{a} : \mathbb{S}_{p^n} \to \mathbb{S}_{p^n}$. Note that $\mathfrak{a}(r(-\mathfrak{b}(x))) = x$ for all $x \in \mathbb{S}_{p^n}$. Finally, they let $\mathbb{S}_{p^n}(h) = \{t \in \mathbb{Z} : h \leq t < h + p^n\}$, and let b denote the unique integer $b \in \mathbb{S}_{p^n}(h)$ such that $\mathfrak{a}(r(b)) = p^n - 1$. For each $x \in \mathbb{S}_{p^n}$, define:

$$d(x) = \left\lfloor \frac{b + \mathfrak{b}(x) - h}{p^n} \right\rfloor;$$

$$w(x) = \min\{d(y + x) - d(y) : y \in \mathbb{S}_{p^n}, y \preceq p^n - 1 - x\};$$

$$\mathcal{D} = \{y \in \mathbb{S}_{p^n} : d(y) > d(y - x) + w(x) \text{ for all } x \in \mathbb{S}_{p^n} \text{ with } 0 \prec x \preceq y\};$$

$$\mathcal{E} = \{y \in \mathbb{S}_{p^n} : w(y) > w(y - x) + w(x) \text{ for all } x \in \mathbb{S}_{p^n} \text{ with } 0 \prec x \prec y\}.$$

The degree p (i.e., $n = 1$ case) gives $\mathfrak{b}(x) = xb$, where b is our ramification number, and thus $d(x) = \left\lfloor \frac{(x+1)b-h}{p} \right\rfloor$. Since the authors choose $b \in \mathbb{S}_{p^n}(h) = \{t \in \mathbb{Z} : h \leq t < h + p^n\}$, this corresponds to $s - p + 1 \leq h \leq s$ for us, in which case $\left\lfloor \frac{b-h}{p} \right\rfloor = 0$, and thus $d(x) = \left\lfloor \frac{(x+1)s-h}{p} \right\rfloor$. Overall, re-writing x as j, we have for $s - p + 1 \leq h \leq s$ and $0 \leq j, u \leq p - 1$:

$$\begin{aligned} d(j) &= \left\lfloor \frac{(j+1)s - h}{p} \right\rfloor; \\ w(j) &= \min\{d(j + i) - d(i) : 0 \leq i \leq p - 1 - j\}; \\ \mathcal{D} &= \{u : d(u) > d(u - j) + w(j) \text{ for all } j \text{ with } 0 < j \leq u\}; \\ \mathcal{E} &= \{u : w(u) > w(u - j) + w(j) \text{ for all } j \text{ with } 0 < j < u\}. \end{aligned} \tag{3.2}$$

Note that we lose no generality by limiting h to $s - p + 1 \leq h \leq s$, but it is convenient for us as $d(0) = 0$ in this case. Note also that, for convenience, we have suppressed the dependence of h in the notation and, by definition, we always have $0 \in \mathcal{D}$ and $0, 1 \in \mathcal{E}$.

Remark 3.3. *[Fer73] defines*

$$\nu_j^{(h)} := \left\lfloor \frac{jt + s - h}{p} \right\rfloor$$

and

$$\eta_j^{(h)} := \min_{0 \leq i \leq p-i-j} (\nu_{j+i}^{(h)} - \nu_i^{(h)})$$

for the char$(K) = 0$ case when $q_0 = 0$. Note, then, that $d(j) = \nu_j^{(h)}$ and $w(j) = m_j^{(h)} = \eta_j^{(h)}$. Note also, in the characteristic 0 case, that, for $b < \frac{pe}{p-1} - 1$,

$\mathcal{A}(\mathfrak{O}_L)$ *is generated by*

$$\left\{\frac{f^i}{\pi^{\eta_i^{(h)}}}\right\}_{0\le i\le p-1},$$

where $f = \sigma - 1$*, which is as we obtained in* (3.1) *for the char*$(K) = p$ *case.*

We now give the analogous result of Theorem 3.2 using our definitions of $\mathcal{D}$ and $\mathcal{E}$. Note that this is also a special case of Theorem 3.4 of [BE13a] for degree p extensions.

Proposition 3.4. *For* $s - p + 1 \le h \le s$*, the minimal number of* $\mathcal{A}(\mathfrak{P}^h)$*-module generators of* $\mathfrak{P}^h$ *is* $|\mathcal{D}|$*, and the embedding dimension* $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ *of* $\mathcal{A}(\mathfrak{P}^h)$ *is* $|\mathcal{E}|$*.*

Proof. By Theorem 3.2 we must have $D^{(h)} = \mathcal{D}$ and $E^{(h)} = \mathcal{E}$. To see this, we will explore the relationship between these two notations $a_j^{(h)}, w_j^{(h)}$ and $d(j), w(j)$:

$$\begin{aligned} a_{p-j-1}^{(h)} &= \left\lceil \frac{(p-j-1)s+h}{p} \right\rceil \\ &= s + \left\lceil \frac{-(j+1)s+h}{p} \right\rceil \\ &= s - \left\lfloor \frac{(j+1)s-h}{p} \right\rfloor \\ &= s - d(j). \end{aligned}$$

Since $m_j^{(h)} = \min_{0\le i<p-j}\{a_{i+j}^{(h)} - a_i^{(h)}\}$, we have:

$$m_j^{(h)} = \min_{0\le i\le p-1-j}\{d(p-1-i) - d(p-1-i-j)\}.$$

Let $i' = p - 1 - i - j$. Then,

$$\begin{aligned} m_j^{(h)} &= \min\{d(i'+j) - d(i') : 0 \le i \le p-1-j\} \\ &= \min\{d(i'+j) - d(i') : 0 \le p-1-i'-j \le p-1-j\} \\ &= \min\{d(i'+j) - d(i') : -(p-1-j) \le -i' \le 0\} \\ &= \min\{d(i'+j) - d(i') : p-1-j \ge i' \ge 0\} \\ &= \min\{d(i'+j) - d(i') : 0 \le i' \le p-1-j\}. \end{aligned}$$

Thus, $m_j^{(h)} = w(j)$.

So now, if we let $u = i - 1$ and $v = j - 1$, then:

$$\begin{aligned}
D^{(h)} &= \{i : 1 \leq i \leq p : a_{p-i} + m_{i-j} < a_{p-j} \text{ for all } j \text{ with } 1 \leq j < i\} \\
&= \{i : 1 \leq i \leq p : s - d(i-1) + m_{i-j} < s - d(j-1) \text{ for all } j \text{ with } 0 \leq j-1 < i-1\} \\
&= \{u : 0 \leq u < p : d(u) > d(v) + w(u-v) \text{ for all } v \text{ with } 0 < v \leq u\}.
\end{aligned}$$

Hence $D^{(h)} = \mathcal{D}$ and $D^{(0)} = D$. Similarly, by simple substitution:

$$\begin{aligned}
E^{(h)} &= \{i : m_j^{(h)} + m_{i-j}^{(h)} < m_i^{(h)} \text{ for all } j \text{ with } 0 < j < i\}. \\
&= \{i : w(i) > w(j) + w(i-j) \text{ for all } j \text{ with } 0 < j < i\}.
\end{aligned}$$

Thus $E^{(h)} = \mathcal{E}$, and $E^{(0)} = E$. $\square$

For the remainder of this discussion, we will return to the $\mathrm{char}(K) = p$ case, for degree p extensions, and use the notation from [BE13a], i.e., we will be considering $d(j)$, $w(j)$, $\mathcal{D}$ and $\mathcal{E}$ with $s-p+1 \leq h \leq s$, in order to investigate the the embedding dimension of $\mathcal{A}(\mathfrak{P}^h)$, and the minimal number of $\mathcal{A}(\mathfrak{P}^h)$-generators (and hence we will also consider the freeness of each $\mathfrak{P}^h$ over its associated order).

Chapter 4

"Words" and Co-ordinates for Degree p Sequences

Recall that we are considering the $\mathrm{char}(K) = p$ case for Galois extensions of degree p. In this chapter we introduce what we term "*words*", and a co-ordinate system, in order to describe the sequence of $d(j)$s in general (i.e., for varying h, s and p). Once we have obtained the description of the $d(j)$s, we will be able to describe the general form of the $w(j)$s, and thus find the sets $\mathcal{D}$ and $\mathcal{E}$.

4.1 The Sequence of $d(j)$s for $h = s$

We shall begin this section with an example. Recall that for general s and p (with $\gcd(s,p) = 1$), the standard continued fraction expansion of $\frac{s}{p}$ is $\frac{s}{p} = [0; q_1, \ldots, q_n]$, with $q_n \geq 2$.

Example 4.1. *Let* $\frac{s}{p} = \frac{5}{13} = [0; 2, 1, 1, 2]$*, also let* $h = s$*. For* $0 \leq j \leq p-1$*, we have* $d(j) = \left\lfloor \frac{(j+1)s-h}{p} \right\rfloor = \left\lfloor \frac{js}{p} \right\rfloor$*. We can work out each value of* $d(j)$ *and* $w(j)$ *(defined in* (3.2)*), as shown in the following table:*

j	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
$d(j)$	*0*	*0*	*0*	*1*	*1*	*1*	*2*	*2*	*3*	*3*	*3*	*4*	*4*
$w(j)$	*0*	*0*	*0*	*1*	*1*	*1*	*2*	*2*	*3*	*3*	*3*	*4*	*4*

In this example note that $d(j) = w(j)$ for all j. This will not always be the case, but we will now show it is a necessary and sufficient condition for freeness, in general. Suppose s and p are such that $w(j) = d(j)$ for all j, and where $s - p + 1 \leq h \leq s$ with $gcd(s, p) = 1$. Then, by (3.2):

$$\begin{aligned}\mathcal{D} &= \{u : d(u) > d(u - j) + w(j) \text{ for all } j \text{ with } 0 < j \leq u\} \\ &= \{u : d(u) > d(u - j) + d(j) \text{ for all } j \text{ with } 0 < j \leq u\}.\end{aligned}$$

We cannot satisfy this inequality for all values of u in the necessary range (except for $u = 0$) as we can always assign $j = u$. Thus $\mathcal{D} = \{0\}$ and $|\mathcal{D}| = 1$ which, by Proposition 3.4, signifies freeness. For completeness, we also calculate the set $\mathcal{E}$ for the above example (via its definition) as $\mathcal{E} = \{0, 1, 3, 8\}$.

Since we are concerned with the size and shape of the sets $\mathcal{D}$ and $\mathcal{E}$ in general, we need a method of describing the sequence of $d(j)$s and $w(j)$s for each h, s and p. In order to do this, it is useful to look at residues: for general s, p, h, let $c(j) = \mathrm{res}_p((j+1)s - h)$ be the least non-negative residue modulo p of $(j+1)s - h$. Then:

$$c(j) = (j + 1)s - h - pd(j).$$

In Example 4.1 above, when $s = 5$, $p = 13$ and $h = s$, the residues are then as follows:

$$|\ 0\ 5\ 10\ |\ 2\ 7\ 12\ |\ 4\ 9\ |\ 1\ 6\ 11\ |\ 3\ 8\ |$$

where a vertical line, |, denotes the ends of what we shall term *blocks*, i.e., the points before which we obtain a value greater than or equal to p by adding s to the previous value of $c(j)$ (which correspond to the points before which $d(j)$ increments by one). In this example there are 5 blocks of lengths 3, 3, 2, 3, 2.

In general, i.e., not just in the above example but still with $h = s$, each block is either "short" (of length $q_1 = \lfloor p/s \rfloor$) or "long" (of length $q_1 + 1$), and there are s blocks in total (one starting with each of the residues $0, \ldots, s-1$). As in Chapter 2, where we discussed the Euclidean Algorithm, we let $p = q_1 s + r_1$, where $0 \leq r_1 \leq s$. There are, therefore, r_1 long blocks and $s - r_1$ short ones. We will write S and L to denote short and long blocks respectively. For instance, the pattern of residues in the example above reads: LLSLS. We shall term particular patterns of blocks as *words* (i.e., an amalgamation of long and short blocks in some, specific order). Words may occur several times in the pattern of residues: in the above example, LS occurs twice, as 2 7 12 | 4 9 and 1 6 11 | 3 8. The entire pattern of residues above is represented by the word $LLSLS = L(LS)^2$ but this will change depending on h,s and p. We therefore need a method of describing these words in general. Let $S_0 = * = L_0$ (a single element of a block) and let

$$S_1 = *^{q_1}, \qquad L_1 = *^{q_1+1}, \tag{4.1}$$

so that L_1 and S_1 are what we just called L and S respectively. Then, for $1 \leq k \leq n$, we define recursively:

$$L_k = L_{k-1}S_{k-1}^{q_k}, \qquad S_k = L_{k-1}S_{k-1}^{q_k-1} \text{ for even } k \geq 2; \tag{4.2}$$

$$L_k = S_{k-1}^{q_k}L_{k-1}, \qquad S_k = S_{k-1}^{q_k-1}L_{k-1} \text{ for odd } k \geq 3. \tag{4.3}$$

We will refer to L_k and S_k as *blocks of level k*.

Theorem 4.2. *If $\frac{s}{p} = [0; q_1, \ldots, q_n]$, with $q_n \geq 2$, then the sequence of residues when $h = s$ gives the word S_n.*

For clarity, we now turn to an example before assembling relevant definitions and lemmata for the proof.

Example 4.3. *As in Example 4.1, let $\frac{s}{p} = \frac{5}{13} = [0; 2, 1, 1, 2]$ and let $h = s$. Then:*

$$\begin{aligned}
S_4 &= L_3S_3^{q_4-1} \\
&= S_2^{q_3}L_2(S_2^{q_3-1}L_2)^{q_4-1} \\
&= (LS^{q_2-1})^{q_3}LS^{q_2}[(LS^{q_2-1})^{q_3-1}LS^{q_2}]^{q_4-1} \\
&= (LS^0)^1LS^1[(LS^0)^0LS^1]^1 \\
&= LLSLS.
\end{aligned}$$

Hence $S_4 = L(LS)^2$, which is the same pattern of residues that we found in Example 4.1, since $L_1 = *^3$ and $S_1 = *^2$.

Remark 4.4. *In the case $h = s$, these words denoting our sequence of residues will always consist of complete - or unbroken - L and S blocks. As we will see later, many values of h lead to broken L and S blocks, which can lead to problems when computing $\mathcal{D}$ and $\mathcal{E}$.*

We now introduce some terminology and notation to allow us to express where a given word W occurs in the pattern of residues. For $0 \leq g < s$, we will say *W fits at g* if, within the sequence of residues (repeated as necessary), the block starting with g begins an occurrence of W. Thus, in Example 4.1, LSL fits at 2 (i.e., 2 7 12 | 4 9 | 1 6 4 occurs in the sequence of residues), and SL fits at both 4 and 3 (i.e., both 4 9 | 1 6 11 and 3 8 | 0 5 10 occur). If two words both fit at the same g, then one is an initial segment of the other.

Definition 4.5. *We attach to each word W a quadruple of integers*

$$[W] = (f(W), m(W), M(W), \mu(W)),$$

where, if an occurrence of the word begins at position j where $c(j) = g$ (with $0 \leq g < s$), and the sequence of residues can be repeated,

- *$g + f(W)$ is the first entry in the block after the occurrence of W (so $f(W)$ is the "total increment" corresponding to the word; note that this can be negative);*

- *$g + m(W)$ is the minimal entry in the occurrence of the word (so $m(W) \leq 0$, and $-m(W)$ is the "depth" of the word below its initial entry);*

- *$g + M(W)$ is the maximal entry in the occurrence of the word (so $M(W) \geq 0$, and $M(W)$ is the "height" of the word above its initial entry);*

- *$g + \mu(W)$ is the smallest of the* final *entries in the blocks making up the occurrence of W.*

Example 4.6. *As in Examples 4.1 and 4.3, let $\frac{s}{p} = \frac{5}{13}$, let $h = s$ and now also let $W = LS$. The residues, as before, are:*

$$| \ 0 \ 5 \ 10 \ | \ 2 \ 7 \ 12 \ | \ 4 \ 9 \ | \ 1 \ 6 \ 11 \ | \ 3 \ 8 \ |.$$

Then $W = LS$ *fits at* g *for* $g = 2$ *(i.e.,* $2\ 7\ 12 \mid 4\ 9$*), and at* $g = 1$ *(i.e.,* $1\ 6\ 11 \mid 3\ 8$*). For the two cases of* g*:*

$$\begin{aligned} 2 + f(LS) &= 1 \quad &\text{and}\quad 1 + f(LS) &= 0;\\ 2 + m(LS) &= 2 \quad &\text{and}\quad 1 + m(LS) &= 1;\\ 2 + M(LS) &= 12 \quad &\text{and}\quad 1 + M(LS) &= 11;\\ 2 + \mu(LS) &= 9 \quad &\text{and}\quad 1 + \mu(LS) &= 8, \end{aligned}$$

the last line is true since, in our two cases of where W *fits, we have blocks ending with* 12 *and* 9*, or* 11 *and* 8*. Clearly* $\min\{12, 9\} = 9$ *and* $\min\{11, 8\} = 8$*. Thus, solving each equation, we obtain:* $[LS] = (f, m, M, \mu) = (-1, 0, 10, 7)$.

The quadruple $[W]$ does not depend on g, but does determine the values of g at which W fits. In particular, we have:

Lemma 4.7.

$$W \textit{ fits at } g \Leftrightarrow \begin{cases} 0 \le g + f(W) < s;\\ g + m(W) \ge 0;\\ g + M(W) < p;\\ g + \mu(W) \ge p - s. \end{cases} \tag{4.4}$$

Proof. Suppose W fits at g. Then, firstly, we have $0 \le g + f(W) < s$, since the start of a block is always less than s, as we are adding on s each time. Secondly, $g+m(W) \ge 0$, as it is the minimal entry in the word (which can never be negative). Thirdly, $g + M(W) < p$, as we are working modulo p, thus the maximal entry in any block must always be less than p. Finally, the condition $g+\mu(W) \ge p-s$ holds true and indicates that we have not incorrectly placed a short block where we could have placed a long block. Conversely, if each of the right hand side conditions hold, then in particular the first entry after the word W is strictly less than s, which indicates that we are not in the middle of a block, but indeed are at the beginning of a block. Since the last condition indicates that we have not placed a short block where we could have placed a long one, then W must fit at g. These conditions, along with the maximal and minimal entry conditions mean that W must fit at g if the right hand side inequalities hold. □

We can also give a formula for the quadruple of the word obtained by concatenating two given words (provided that they can indeed occur consecutively):

Lemma 4.8. *If*

$$[W] = (f, m, M, \mu), \qquad [W'] = (f', m', M', \mu'),$$

then

$$[WW'] = (f + f', \min(m, f + m'), \max(M, f + M'), \min(\mu, f + \mu')). \tag{4.5}$$

Proof. To see this, look at the first entry: $f + f'$. By definition we need $g + f + f'$ to be the first entry after the word WW', which is the same as saying the first entry after the word W'. Note that $g + f$ is the first entry after W, which will be the same value as g' (since the words directly follow on from each other). Thus $g+f+f' = g'+f'$, which is the first entry in the block after W', as desired. Similarly, the second entry of the quadruple implies that we need $g + m$ or $g + f + m'$ to be the minimal entry occurring in WW'. Clearly $g + m$ will be the minimal entry in the occurrence of WW' if the minimal entry occurs in W. If, however, the minimal entry occurs in W', then the minimal entry will be $g' + m' = g + f + m'$ since, as above, $g + f = g'$. Therefore, the second entry of the quadruple is $\min(m, f + m')$. The other entries of the quadruple follow by similar arguments. □

We may now prove Theorem 4.2.

Proof of Theorem 4.2. Recall from the Euclidean Algorithm in Chapter 2, we have remainders r_j, where: $r_{j-2} = q_j r_{j-1} + r_j$ with $0 \leq r_j < r_{j-1}$. We now prove the assertion of the Theorem by induction, simultaneously with the following formulae:

$$[S_k] = (-r_k, 0, p - r_k - r_{k-1}, p - s - r_k) \text{ for odd } k; \tag{4.6}$$

$$[L_k] = (r_{k-1} - r_k, 0, p - r_k, p - s + r_{k-1} - r_k) \text{ for odd } k; \tag{4.7}$$

$$[S_k] = (r_k, 0, p - r_{k-1}, p - s + r_k) \text{ for even } k; \tag{4.8}$$

$$[L_k] = (r_k - r_{k-1}, 0, p - r_{k-1}, p - s + r_k - r_{k-1}) \text{ for even } k. \tag{4.9}$$

First consider the case $k = 1$. If $n = 1$, we have $s = 1$ and $q_1 = p$. So the pattern of residues is a single short block of length q_1. Thus the pattern is given by the word

$S = S_1$. Now let $n > 1$, (or, equivalently, $s > 1$). In this case the first block is long, starting with 0 and ending with $q_1 s$, so the pattern starts with the word $L = L_1$. We now check (4.7) and (4.6). We have $f(L) = (q_1+1)s-p = s-r_1 = r_0-r_1$ since $p = q_1 s + r_1$ and $r_0 = s$. Also $f(S) = q_1 s - p = -r_1$. Clearly $m(L) = m(S) = 0$, $M(L) = q_1 s = p - r_1 = \mu(L)$ and $M(S) = (q_1 - 1)s = p - r_1 - s = \mu(S)$. Thus (4.7) and (4.6) hold for $k = 1$.

We next give the induction step for even k. If we reach step k, we must have $n \geq k$ and hence $r_{k-1} > 0$. From the induction hypothesis, we have

$$[S_{k-1}] = (-r_{k-1}, 0, p - r_{k-1} - r_{k-2}, p - s - r_{k-1}), \tag{4.10}$$

$$[L_{k-1}] = (r_{k-2} - r_{k-1}, 0, p - r_{k-1}, p - s + r_{k-2} - r_{k-1}),$$

since $k - 1$ is odd. Using (4.5) and a further induction, it follows that, for $\alpha \geq 1$, we have

$$[L_{k-1}S_{k-1}^{\alpha-1}] = (r_{k-2} - \alpha r_{k-1}, 0, p - r_{k-1}, p - s + r_{k-2} - \alpha r_{k-1}).$$

Thus, since $r_{k-2} - q_k r_{k-1} = r_k \geq 0$, it follows from (4.4) - in particular the fourth condition - that the word $L_{k-1}S_{k-1}^{\alpha-1}$ fits at 0 if $\alpha = q_k$, but not if $\alpha = q_k + 1$. In particular, the word $S_k = L_{k-1}S_{k-1}^{q_k-1}$ fits at 0 (so it forms an initial segment of the word given by the pattern of residues), and we have

$$[S_k] = (r_k, 0, p - r_{k-1}, p - s + r_k),$$

giving (4.8) for k. Finally, if $n = k$, we have $f(S_k) = r_k = 0$, so that S_k is the word for the complete pattern of residues. Similarly, we note for k even, $L_k = L_{k-1}S_{k-1}^{q_k} = S_k S_{k-1}$. Then, using (4.5), (4.8) and (4.10), we have:

$$[L_k] = (r_k - r_{k-1}, 0, \max(p - r_{k-1}, r_k + p - r_{k-1} - r_{k-2}), \min(p - s + r_k, r_k + p - s - r_{k-1})),$$

which simplifies to (4.9), as required. This gives Theorem 4.2 for $n = k$ even.

Now suppose that $k \geq 3$ is odd. By the induction hypothesis we have:

$$[L_{k-1}] = (r_{k-1} - r_{k-2}, 0, p - r_{k-2}, p - s + r_{k-1} - r_{k-2}).$$

Using the induction hypothesis and (4.5) we have, for $\alpha \geq 2$:

$$[S_{k-1}^{\alpha-1}] = ((\alpha-1)r_{k-1}, 0, p - r_{k-2} - (\alpha-2)r_{k-1}, p - s + r_{k-1}).$$

Taking $\alpha = q_k$, and using (4.5) again, we obtain:

$$[S_{k-1}^{q_k-1}L_{k-1}] = (q_k r_{k-1} - r_{k-2}, 0, p - r_{k-2} + (q_k-1)r_{k-1}, (q_k-1)r_{k-1} + p - s + r_{k-1} - r_{k-2})$$

which, since $r_{k-2} - q_k r_{k-1} = r_k$, simplifies to:

$$[S_k] = (-r_k, 0, p - r_k - r_{k-1}, p - s - r_k),$$

and which agrees with (4.6). Moreover, if $k = n$ (so $r_k = 0$) then, by (4.4), S_k fits at 0 and gives the complete pattern of residues. Similarly, for k odd, we have $L_k = S_{k-1}^{q_k}L_{k-1} = S_{k-1}S_k$. Then by (4.5), (4.6) and the induction hypothesis for $[S_{k-1}]$, we have:

$$[L_k] = (r_{k-1} - r_k, 0, \max(p - r_{k-2}, p - r_k), \min(p - s + r_{k-1}, r_{k-1} + p - s - r_k)),$$

which simplifies to (4.7), as required. This completes the induction for odd k, and the proof of Theorem 4.2.

□

We can also easily calculate the length of these words. Let $|S_k|$ denote the length of the word S_k and define $s_k := |S_k|$, and $l_k := |L_k|$. From equations (4.1) to (4.3) we clearly see that:

$$l_k = s_k + s_{k-1} \quad \text{for } k \geq 1. \tag{4.11}$$

We claim:

$$s_k = q_k s_{k-1} + s_{k-2} \quad \text{for } k \geq 2, \tag{4.12}$$

with $s_0 = 1$, $s_1 = q_1$ and $s_n = p$. Equation (4.12) can be proved by a simple induction. Assume it holds for k. Then, by (4.2) and (4.3):

$$s_{k+1} = s_k(q_{k+1} - 1) + l_k.$$

By (4.11) this becomes:

$$s_{k+1} = s_k \cdot q_{k+1} + s_{k-1}.$$

We conclude the induction by noting in particular that when $k = 2$, we obtain $s_2 = q_2 s_1 + s_0 = q_1 q_2 + 1 = |S_2|$, where $S_2 = LS^{q_2 - 1}$. Finally, we note that $s_n = p$, since s_n is the length of the entire word describing the pattern of the $\{d(j)\}_{0 \le j \le p-1}$. We will use (4.11) and (4.12) later, in Chapter 5.

Now that we have a method for describing the pattern of residues, and hence the $d(j)$s when $h = s$, we need to find a method for describing the pattern of $d(j)$s for every value of h in our prescribed range. To do this, we will invent a co-ordinate system.

4.2 Co-ordinate System

We introduce a string of x_i for $i = 1, \dots n$, which we shall term *co-ordinates* and denote as $(x_1, \dots, x_n)$. We would like these co-ordinates to describe the pattern of the $\{d(j)\}_{0 \le j \le p-1}$ as h varies. So a given value of h (and thus a given pattern of $\{d(j)\}$) will have a corresponding co-ordinate. For instance, we would like to obtain a pattern such as:

$s - h$	Co-ord
0	$(0, \dots, 0, 0)$
1	$(0, \dots, 0, 1)$
$\vdots$	$\vdots$
$q_n - 1$	$(0, \dots, 0, q_n - 1)$
q_n	$(0, \dots, 0, 1, 0)$
$q_n + 1$	$(0, \dots, 0, 1, 1)$
$\vdots$	$\vdots$
$2q_n$	$(0, \dots, 0, 2, 0)$
$2q_n + 1$	$(0, \dots, 0, 2, 1)$
$\vdots$	$\vdots$
$q_{n-1}q_n$	$(0, \dots, 0, q_{n-1}, 0)$
$q_{n-1}q_n + 1$	$(0, \dots, 0, 1, 0, 1)$
$\vdots$	$\vdots$

and so on. Note that:

- $0 \le x_i \le q_i$; and
- if $x_i = q_i$, then $\{i < n$ and $x_{i+1} = 0\}$.

Indeed, we shall call a set of co-ordinates *valid* if they satisfy the above two properties.

If we let f_j be the number of valid co-ordinates with $x_i = 0$ for all $i < j$. Then:

$$f_{n+1} = 1, \quad f_n = q_n.$$

We can also calculate f_{j-1} in terms of f_j and f_{j+1} (for $1 < j \le n$): we have q_{j-1} ways of choosing x_{j-1} (with $0 \le x_{j-1} < q_{j-1}$), each of which can be followed by f_j choices for $x_j, x_{j+1}, \dots, x_n$. We also have to add on the case when $x_{j-1} = q_{j-1}$, but in this situation we have $x_j = 0$, and there are f_{j+1} choices for $x_{j+1}, \dots, x_n$. Thus:

$$f_{j-1} = q_{j-1} f_j + f_{j+1}.$$

Now that we have a way of counting the number of co-ordinates with zeros preceding a particular co-ordinate x_i, we are in a position to obtain the value of $s - h$ from a given co-ordinate. For example, when $n = 2$, we find $s - h$ by multiplying the number of co-ordinates of the form $(0, x_2)$ with the particular value of x_1 we are at. Finally, we add on the current value of x_2, i.e.,

$$\begin{aligned} s - h &= x_1 f_2 + x_2 \\ &= q_2 x_1 + x_2. \end{aligned}$$

In the same way, for general n, we can write:

$$s - h = x_1 f_2 + x_2 f_3 + \ldots + x_{n-1} f_n + x_n f_{n+1}.$$

We now give an interpretation of the f_i in terms of the continued fraction expansion. Let $Y_j = [0; q_j, \dots, q_n]$, $(1 \le j \le n)$ i.e., the truncated version of our continued fraction expansion. Then:

$$Y_j = \frac{1}{q_j + Y_{j+1}}.$$

We claim $Y_j = \frac{f_{j+1}}{f_j}$. This is clearly true for $j = n$. If it is true for $j + 1$ then:

$$Y_j = \frac{f_{j+1}}{f_{j+1}q_j + f_{j+2}} = \frac{f_{j+1}}{f_j}.$$

So our claim is true, by induction. Then:

$$\frac{s}{p} = Y_1 = \frac{f_2}{f_1}.$$

This implies $p = f_1$ and $s = f_2$, as we are dealing with positive integers, and s and p have no common factors. Therefore, $s - h$ becomes:

$$s - h = x_1 s + x_2 f_3 \ldots + x_{n-1} q_n + x_n. \tag{4.13}$$

Writing $s - h$ in this way describes the corresponding sequence of $\{d(j)\}$ - which we will state formally in Theorem 4.13. Before we state that theorem, however, we look at the following proposition:

Proposition 4.9. *For* $1 \leq j \leq n + 1$,

$$s_{n-1} f_j \equiv (-1)^{n+j-1} s_{j-2} \pmod{p}.$$

In particular,

$$s_{n-1} s = s_{n-2} f_2 \equiv (-1)^{n-1} s_0 = (-1)^{n-1} \pmod{p}. \tag{4.14}$$

Proof. For $j = n + 1$:

$$s_{n-1} f_{n+1} = s_{n-1} = (-1)^{n+(n+1)-1} s_{n-1}.$$

For $j = n$:

$$\begin{aligned} s_{n-1} f_n &= s_{n-1} q_n \\ &= s_n - s_{n-2} \\ &= p - s_{n-2} \\ &\equiv (-1)^{n+(n-1)} s_{n-2} \pmod{p}. \end{aligned}$$

For $1 \leq j \leq n - 1$, we use downwards induction. Assuming the formula for $j + 1$ and $j + 2$:

$$\begin{aligned} s_{n-1}f_j &= s_{n-1}(f_{j+2} + q_j f_{j+1}) \\ &\equiv (-1)^{n-1+j+2}s_j + (-1)^{n-1+j+1}q_j s_{j-1} \pmod p \\ &\equiv (-1)^{n+j-1}[s_j - q_j s_{j-1}] \pmod p \\ &\equiv (-1)^{n+j-1}s_{j-2} \pmod p. \end{aligned}$$

□

For the sequence $d(j) = \left\lfloor \frac{s(j+1)-h}{p} \right\rfloor = \left\lfloor \frac{js+(s-h)}{p} \right\rfloor$, increasing $s-h$ by 1 means shifting the sequence $\{s^{-1} \bmod p\}$ symbols from left to right. By (4.14),

$$s^{-1} \equiv \begin{cases} -s_{n-1} & \text{if } n \text{ even} \\ s_{n-1} & \text{if } n \text{ odd.} \end{cases}$$

Thus we must move s_{n-1} - i.e., the length of the string S_{n-1} - from right to left (left to right) if n is even (odd). This motivates the following Algorithm:

Algorithm 4.10. ***For even*** *n:*

Step 1. Start with $S_n = L_{n-1}S_{n-1}^{q_n-1}$.

Step 2. Move x_n *copies of* S_{n-1} *right to left.*

Step 3. Then move x_{n-1} *copies of* S_{n-2} *left to right.*

Step 4. Then move x_{n-2} *copies of* S_{n-3} *right to left.*

$\vdots$

Step $n+1$. *Conclude by moving* x_1 *copies of* $S_0 = *$ *left to right.*

For odd *n:*

Step 1. Start with $S_n = S_{n-1}^{q_n-1}L_{n-1}$.

Step 2. Move x_n *copies of* S_{n-1} *left to right.*

Step 3. Then move x_{n-1} *copies of* S_{n-2} *right to left.*

Step 4. Then move x_{n-2} *copies of* S_{n-3} *left to right.*

$$\vdots$$

Step $n+1$. *Conclude by moving* x_1 *copies of* $S_0 = *$ *left to right.*

We illustrate how this Algorithm works with the following example. Then, in Theorem 4.13, we will prove that the string resulting from this Algorithm is the one which corresponds to the sequence $\{d(j)\}$ for co-ordinates $(x_1, \ldots, x_n)$.

Example 4.11. *Let* $\frac{9}{29} = [0; 3, 4, 2]$. *In this case* $n = 3$. *By* (4.1), (4.2) *and* (4.3), *we have* $S_3 = S_2L_2$, *where* $S_2 = L_1S_1S_1S_1$, $L_2 = L_1S_1S_1S_1S_1$, $S_1 = * * *$, *and* $L_1 = * * * *$. *Take the example when we have co-ordinates* $(1, 2, 1)$. *Our algorithm goes as follows:*

- *start with* $S_3 = S_2L_2$. *Then move* $x_3 = 1$ *lots of* S_2 *from left to right. This gives us* L_2S_2 *which we can write as* $L_2L_1S_1S_1S_1$.
- *Now move* $x_2 = 2$ *lots of* S_1 *from right to left, giving us* $S_1S_1L_2L_1S_1$.
- *Finally, move* $x_1 = 1$ *lots of* $*$ *from left to right, giving us* $* * S_1L_2L_1S_1*$.

Proposition 4.12. *For* $1 \leq i \leq n$, *we have* $x_i \leq q_i$ *with*

$$x_i = q_i \quad \Rightarrow \quad x_{i+1} = 0.$$

In particular, $x_n < q_n$.

Proof. For $i = n$ clearly, for either even or odd n, $x_n < q_n$ since there are only $q_n - 1$ blocks of S_{n-1} in the word S_n. For $i < n$, there will always be an L_{n-i} block on the opposite side of the word if we didn't move any S_{n-j-1} blocks (i.e., if $x_{i+1} = 0$). So if we are able to move q_i blocks, we must have not moved any short level i blocks in the previous step, in order for there to be a long level i block (and hence q_i level $i-1$ short blocks) on the appropriate end of the word. $\square$

Theorem 4.13. *To obtain the sequence* $\{d(j)\}$ *for* $s-h = x_1f_2+\ldots+x_nf_{n+1}$, *i.e., for co-ordinates* $(x_1, \ldots, x_n)$, *perform Algorithm 4.10. At each stage, the remaining pattern starts/ends with enough copies of* S_k *for the required move to be possible. In fact, when we are about to move* x_k *copies of* S_{k-1} *we have:*

for k even, the pattern ends with:

$$\begin{cases} L_k = L_{k-1}S_{k-1}^{q_k} & \text{if } k < n \text{ and } x_{k+1} = 0 \\ S_k = L_{k-1}S_{k-1}^{q_k-1} & \text{otherwise.} \end{cases} \tag{4.15}$$

The pattern starts with L_{k-1}.

For k odd, the pattern ends with L_{k-1} and starts with:

$$\begin{cases} L_k = S_{k-1}^{q_k}L_{k-1} \text{ if } x_{k+1} = 0 \\ S_k = S_{k-1}^{q_k-1}L_{k-1} \text{ otherwise.} \end{cases} \tag{4.16}$$

Proof. We show by downward induction on $k \leq n$ that statement is true if $x_1 = \ldots = x_k = 0$. For $k = n$ we have $s - h = 0$, and the string is just $S_n = L_{n-1}S_{n-1}^{q_n-1}$ for n even - so (4.15) holds - and $S_n = S_{n-1}^{q_n-1}L_{n-1}$ for n odd - so (4.16) holds. Now suppose $k > 0$ and we are about to move x_k copies of S_{k-1} according to Algorithm 4.10 (i.e., the moves for $x_{k+1}, \ldots x_n$ have already been done). Thus we are increasing $s - h$ from $x_{k+1}f_{k+2} + \ldots + x_nf_{n+1}$ to $x_kf_{k+1} + \ldots + x_nf_{n+1}$, i.e., increasing $s-h$ by x_kf_{k+1}. This corresponds to moving $\pm s_{k-1}x_k$ symbols from right to left, since by Proposition 4.9:

$$s_{n-1}x_kf_{k+1} \equiv (-1)^{n+k}x_ks_{k-1} \equiv \begin{cases} x_ks_{k-1} \pmod p & \text{for } k \text{ even} \\ -x_ks_{k-1} \pmod p & \text{for } k \text{ odd.} \end{cases} \tag{4.17}$$

So moving x_k copies of S_{k-1} right to left (for n even) and left to right (for n odd) does indeed give the correct pattern for a new $s - h$. Moreover, this move is actually possible by (4.15) (and (4.16) respectively) since, if $x_k = q_k$, we must have $x_{k+1} = 0$ with $k < n$. Furthermore, if $x_k = 0$ and n is even, then the string starts $S_{k-1}^{x_k}L_{k-1} = L_{k-1} = S_{k-2}^{q_{k-1}}L_{k-2}$ and if $x_k \neq 0$, the string starts with $S_{k-1} = S_{k-2}^{q_{k-1}-1}L_{k-2}$. Still for n even, the string ends with either $L_{k-1} = S_{k-2}^{q_{k-1}}L_{k-2}$ or $S_{k-1} = S_{k-2}^{q_{k-1}-1}L_{k-2}$, and hence ends in L_{k-2} in both cases. Hence (4.16) holds for the odd number $k - 1$. This completes the induction step for k even.

If $x_k = 0$ and n is odd, then the string ends with $L_{k-1}S_{k-1}^{x_k} = L_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}}$ or $S_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}-1}$ otherwise. The string starts with $L_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}}$ or

$S_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}-1}$, so it starts with L_{k-2} in both cases. Thus (4.15) holds for the even number $k-1$. This completes the induction step for k odd.

Now suppose k is odd (respectively even) and we are about to move x_k copies of S_{k-1} left to right (respectively right to left) with (4.16) (respectively (4.15)) holding for k.

Increasing $s-h$ by $x_k f_{k+1}$ corresponds to moving $-x_k$ copies of S_{k-1} right to left (respectively left to right), i.e., $+x_k$ copies of S_{k-1} left to right (respectively right to left). By (4.16) (respectively (4.15)) this move is possible since $x_k < q_k$ unless $x_{k+1} = 0$. If $x_k = 0$, the new string ends (starts) with L_{k-1}, otherwise it ends (starts) with S_{k-1}. For n even, the new string starts with either $S_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}-1}$ or $L_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}}$. So it starts with L_{k-2} and hence (4.15) holds for the even number $k-1$. For n odd, the new string ends with either $S_{k-1} = S_{k-2}^{q_{k-1}-1}L_{k-2}$ or $L_{k-1} = L_{k-2}S_{k-2}^{q_{k-1}}$, so it always ends with L_{k-2} and (4.16) holds for the odd number $k-1$. This concludes the induction step for k odd (even), and concludes the proof of our theorem for general n. $\square$

Example 4.14. *As in Example 4.11, let* $\frac{9}{29} = [0; 3, 4, 2]$. *From what we found in that example, we now know the shape of the* $\{d(j)\}_{0 \leq j \leq p-1}$ *pattern corresponding to the co-ordinate* $(1, 2, 1)$ *in this example is* $**S_1 L_2 L_1 S_1 *$. *In a similar manner, we can obtain the pattern of the various* $\{d(j)\}$*s, for a particular value of* $s-h$*:*

$s-h$	$\{d(j)\}$	*Co-ord*
0	S_2L_2	$(0,0,0)$
1	L_2S_2	$(0,0,1)$
2	$S_1S_2S_2$	$(0,1,0)$
3	$S_1L_2L_1S_1S_1$	$(0,1,1)$
4	$S_1S_1S_2L_1S_1S_1$	$(0,2,0)$
5	$S_1S_1L_2L_1S_1$	$(0,2,1)$
6	$S_1S_1S_1S_2L_1S_1$	$(0,3,0)$
7	$S_1S_1S_1L_2L_1$	$(0,3,1)$
8	$S_1S_1S_1S_1S_2L_1$	$(0,4,0)$
9	$***S_1S_1S_1L_2*$	$(1,0,0)$
10	$***S_1S_1S_1S_1S_2*$	$(1,0,1)$
11	$**S_2S_2*$	$(1,1,0)$
12	$**L_2L_1S_1S_1*$	$(1,1,1)$
13	$**S_1S_2L_1S_1S_1*$	$(1,2,0)$
14	$**S_1L_2L_1S_1*$	$(1,2,1)$
15	$**S_1S_1S_2L_1S_1*$	$(1,3,0)$
16	$**S_1S_1L_2L_1*$	$(1,3,1)$
17	$**S_1S_1S_1S_2L_1*$	$(1,4,0)$
18	$**S_1S_1S_1L_2**$	$(2,0,0)$
19	$**S_1S_1S_1S_1S_2**$	$(2,0,1)$
20	$*S_2S_2**$	$(2,1,0)$
21	$*L_2L_1S_1S_1**$	$(2,1,1)$
22	$*S_1S_2L_1S_1S_1**$	$(2,2,0)$
23	$*S_1L_2L_1S_1**$	$(2,2,1)$
24	$*S_1S_1S_2L_1S_1**$	$(2,3,0)$
25	$*S_1S_1L_2L_1**$	$(2,3,1)$
26	$*S_1S_1S_1S_2L_1\ **$	$(2,4,0)$
27	$*S_1S_1S_1L_2\ ***$	$(3,0,0)$
28	$*S_1S_1S_1S_1L_1S_1S_1S_1***$	$(3,0,1)$

Corollary 4.15. *Let D denote the general pattern of the $\{d(j)\}_{0\leq j\leq p-1}$ for a given n. For $\frac{s}{p}=[0;q_1,\ldots,q_n]$ and co-ordinates $(x_1,\ldots x_n)$ - provided, for all i, $x_i\neq 0$ - the pattern of the Ds for general n are as follows:*

For even n:

$$\begin{aligned} D = {*}^{q_1-x_1}\, & S_1^{x_2-1}S_2^{q_3-x_3-1}L_2S_3^{x_4-1}S_4^{q_5-x_5-1}L_4\ldots \\ & S_{n-2}^{q_{n-1}-x_{n-1}-1}L_{n-2}S_{n-1}^{x_n-1}L_{n-1}S_{n-1}^{q_n-x_n-1}\ldots \\ & L_5S_5^{q_6-x_6-1}S_4^{x_5-1}L_3S_3^{q_4-x_4-1}S_2^{x_3-1}L_1S_1^{q_2-x_2-1}\,{*}^{x_1}\,. \end{aligned} \tag{4.18}$$

For odd n:

$$\begin{aligned} D = {*}^{q_1-x_1}\, & S_1^{x_2-1}S_2^{q_3-x_3-1}L_2S_3^{x_4-1}S_4^{q_5-x_5-1}L_4\ldots \\ & S_{n-2}^{x_{n-1}-1}S_{n-1}^{q_n-x_n-1}L_{n-1}S_{n-1}^{x_n-1}L_{n-2}S_{n-2}^{q_{n-1}-x_{n-1}-1}\ldots \\ & L_5S_5^{q_6-x_6-1}S_4^{x_5-1}L_3S_3^{q_4-x_4-1}S_2^{x_3-1}L_1S_1^{q_2-x_2-1}\,{*}^{x_1}\,. \end{aligned} \tag{4.19}$$

In this chapter we formulated *words* to describe the pattern of the $\{d(j)\}_{0\leq j\leq p-1}$ for all values $s-p+1\leq h\leq s$, via a co-ordinate system $(x_1,\ldots,x_n)$. In the next chapter we aim to describe the $\{w(j)\}_{0\leq j\leq p-1}$ (the definition of which, recall, depended on these $d(j)$) so that we will be able to describe the sets $\mathcal{D}$ and $\mathcal{E}$, and thus realise the complexity of $\mathfrak{P}_L^h$ and $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$.

Chapter 5

Investigating $\mathcal{D}$ and $\mathcal{E}$

As before, let $\frac{s}{p} = [0; q_1, \ldots, q_n]$ and $s - p + 1 \leq h \leq s$. Now recall the following definitions, for $0 \leq i < p$:

$$d(i) = d^{(h)}(i) = \left\lfloor \frac{si + (s-h)}{p} \right\rfloor;$$

$$w(i) = \min\{d(u+i) - d(u) \ : \ 0 \leq u < p - i\}.$$

$$\mathcal{D} = \{u : d(u) > d(u-j) + w(j) \text{ for all } j \text{ with } 0 < j \leq u\};$$

$$\mathcal{E} = \{u : w(u) > w(u-j) + w(j) \text{ for all } j \text{ with } 0 < j < u\}.$$

From now on, we shall denote the string of the $\{w(i)\}_{0 \leq i \leq p-1}$ as W, and the string of the $\{d(i)\}_{0 \leq i \leq p-1}$ as D. We shall talk about these as D and W-strings.

This chapter, then, gives the main results of this thesis: in it we describe the pattern of the W-strings for arbitrary s, p (and hence n) and h in order to describe the sets $\mathcal{D}$ and $\mathcal{E}$. We begin by stating some properties of the D-string.

5.1 Some properties of the D-string

Proposition 5.1. *Fix i with $0 \leq i \leq p-1$. For $0 \leq u < p - i$, we have*

$$d(u+i) - d(u) = \left\lfloor \frac{is}{p} \right\rfloor \ \text{ or } \ \left\lceil \frac{is}{p} \right\rceil.$$

In particular, as u varies, the value of $d(u+i) - d(u)$ can vary by at most 1. Moreover

$$w(i) = \left\lfloor \frac{is}{p} \right\rfloor \ \text{ or } \ \left\lceil \frac{is}{p} \right\rceil.$$

(Proof is immediate.)

Remark 5.2. *The value of* $w(i+u)-w(u)$ *may vary by more than* 1*. For example, if we take* $\frac{s}{p}=\frac{3}{7}=[0;2,3]$ *with* $h=s$*, then we have:*

i	0	1	2	3	4	5	6
$d(i)$	0	1	1	1	2	2	2
$w(i)$	0	0	0	1	1	2	3

and we can see that $w(6)-w(4)=2$*, while* $w(2)-w(0)=0$*.*

Corollary 5.3. *Suppose* $1 \leq q \leq p-1$ *and the* W*-string is a* D*-string up to* q*, that is, for some* h' *we have*

$$w(i)=\left\lfloor \frac{si+s-h'}{p} \right\rfloor \text{ for } 0 \leq i \leq q.$$

Then

(i) $q \in \mathcal{E} \Leftrightarrow w(i)+w(q-i)=w(q)-1$ *whenever* $0<i<q$*. (Since we always have* $w(1)=0$*, this condition implies* $w(q)=w(q-1)+1$*.)*

(ii) $q \in \mathcal{D} \Leftrightarrow w(i)+d(q-i)=w(q)=d(q)-1$ *for* $0<i \leq q$*,*

Proof. (i) Since $w(0)=0$, the definition of $\mathcal{E}$ can be restated as

$$q \in \mathcal{E} \Leftrightarrow w(i)-w(0)<w(q)-w(q-i) \text{ for } 0<i<q.$$

But the segment of the W-string up to position q satisfies the condition in Proposition 5.1, so that

$$w(i)-w(0)<w(q)-w(q-i) \Leftrightarrow w(i)-w(0)=w(q)-w(q-i)-1$$

for each i.

(ii) Recall that, by definition,

$$q \in \mathcal{D} \Leftrightarrow w(i)+d(q-i)<d(q) \text{ for } 0<i \leq q.$$

In particular, as $d(0) = 0$, if $q \in \mathcal{D}$ and $q \geq 1$ then $w(q) < d(q)$. Since both the D-string and the W-string satisfy the condition in Proposition 5.1, the condition $w(q) < d(q)$ is equivalent to $w(q) = d(q) - 1$. Moreover, if $w(q) < d(q)$, we have

$$\begin{aligned} q \in \mathcal{D} \quad &\Leftrightarrow \quad w(i) + d(q-i) < d(q) + w(0) \text{ for } 0 < i \leq q \\ &\Leftrightarrow \quad w(i) - w(0) < d(q) - d(q-i) \text{ for } 0 < i \leq q \\ &\Leftrightarrow \quad w(i) - w(0) = w(q) - d(q-i) - 1 \text{ for } 0 < i \leq q. \end{aligned}$$

□

Note that Corollary 5.3(i) relates the W-string in the forwards and backwards directions at elements of $\mathcal{E}$, while (ii) relates the W-string (forwards) to the D-string (backwards) at elements of $\mathcal{D}$.

We write

$$d_0(j) = \left\lfloor \frac{si}{p} \right\rfloor,$$

for the D-sequence for the ideal $h = s$, with corresponding string S_n. This string has the palindromic property:

Proposition 5.4. *For $0 < i < p$ we have*

$$d_0(i) + d_0(p-i) = s - 1.$$

Thus, in particular, $d_0(i) + d_0(p-i)$ is independent of i (provided $i > 0$).

Proof.

$$d(i) + d(p-i) = \left\lfloor \frac{si}{p} \right\rfloor + \left\lfloor \frac{s(p-i)}{p} \right\rfloor = \left\lfloor \frac{si}{p} \right\rfloor + s + \left\lfloor \frac{-si}{p} \right\rfloor = s - 1$$

since $p \nmid (si)$. □

If we expand S_n in terms of level 1 blocks $S = S_1$ and $L = L_1$, Proposition 5.4 says that the resulting string is almost palindromic. It is not completely palindromic as $i = 0$ is excluded. For $n \geq 2$ (whether even or odd), S_n starts with L_1 and ends with S_1. Proposition 5.4 says that reversing the string of S_1's and L_1's merely swaps these two end symbols. (For $n = 1$, the string S_1 is just a single block S_1 of length $q_1 = p$.)

We say the first q positions in the W-string *form an S-string* if

$$w(i) = \left\lfloor \frac{ti}{q} \right\rfloor \text{ for } 0 \le i < q,$$

where $t = w(q)$ (so the formula holds for $i = q$ as well). Thus the first q characters of the W-string coincide with the S_m-string for $\frac{t}{q}$, where m is the length of the continued fraction expansion of $\frac{t}{q}$.

We now show that if an initial segment of a D-string (for $\frac{s}{p}$ and any ideal h') has the palindromic property then it must be an S-string.

Proposition 5.5. *Suppose that we have some $2 \le q < p$ and that the W-string coincides with the D-string for some ideal h', up to position q, i.e.,*

$$w(i) = \left\lfloor \frac{si + (s - h')}{p} \right\rfloor \text{ for } 0 \le i \le q.$$

Let $t = w(q)$. Then the condition

$$w(i) + w(q - i) = t - 1 \quad \text{for all } i \text{ with } 0 < i < q$$

is equivalent to

$$w(i) = \left\lfloor \frac{ti}{q} \right\rfloor \text{ for } 0 \le i \le q.$$

Proof. We have

$$w(i) = \frac{is + c_0 - c_i}{p}$$

where c_i is the least non-negative residue of $si + (s - h') \bmod p$. In particular, $0 \le c_i < p$ for $0 < i < p$, and $c_0 = s - h'$. So if

$$w(i) + w(q - i) = t - 1 \text{ for all } i \text{ with } 0 < i < q,$$

we have

$$t = \frac{qs + c_0 - c_q}{p}$$

and, for $0 < i < q$,

$$t - 1 = \frac{is + c_0 - c_i}{p} + \frac{(q - i)s + c_0 - c_{q-i}}{p} = \frac{qs}{p} + \frac{2c_0 - c_i - c_{q-i}}{p},$$

so that

$$c_i + c_{q-i} = c_q + c_0 + p \quad \text{for } 0 < i < q. \tag{5.1}$$

Thus, for $0 < i < q$, we have

$$\begin{aligned}\frac{ti}{q} &= \left(\frac{s}{p} - \frac{c_q - c_0}{pq}\right) i \\ &= w(i) + \frac{c_i - c_0}{p} - \frac{(c_q - c_0)i}{pq} \\ &= w(i) + \frac{A(i)}{pq}\end{aligned}$$

where

$$A(i) = q(c_i - c_0) - i(c_q - c_0).$$

Now, as $t = w(q) = w(i) + w(q-i) + 1$, we have $A(i) + A(q-i) = pq$. Thus, if we can show that $A(i) > 0$ whenever $0 < i < q$, we will have $0 < A(i) < pq$ and hence $\left\lfloor \frac{ti}{q} \right\rfloor = w(i)$, as required. Using (5.1) to eliminate c_q, we obtain

$$A(i) = (q-i)c_i + i(p - c_{q-i}) + (2i - q)c_0,$$

which gives $A(i) > 0$ if $2i \geq q$. On the other hand, using (5.1) to eliminate c_0 gives

$$A(i) = ic_i + (p - c_{q-i})(q-i) + (q - 2i)c_q$$

which gives $A(i) > 0$ if $2i \leq q$. Thus $A(i) > 0$ in all cases. □

Now that we have covered some properties of the D-string, we aim to describe the general pattern of the W-strings.

5.2 The Pattern of the W-strings

We seek to show the following things.

1. Algorithm 4.10 tells us that we can always write the D-string for parameters $q_1, \ldots, q_n$ and $x_1, \ldots, x_n$ in the form

$$D_n = d_1^+ d_2^+ \ldots d_n^+ d_n^- \ldots d_1^- = \widetilde{d}_{n-1}^+ d_n^+ d_n^- \widetilde{d}_{n-1}^-$$

   where d_n^+, d_n^- consist of unbroken S_{n-1} and L_{n-1}-blocks, and $\widetilde{d}_{n-1}^+ \widetilde{d}_{n-1}^-$ is either the empty string (if no level $n-1$ block in S_n is broken to form D);

or the D-string for parameters $q_1, \ldots, q_{n-1}$ and $x_1, \ldots, x_{n-1}$ (if an S_{n-1} block is broken, or in one **exceptional case**, when an L_{n-1} block is broken in forming the D-string but is reconstituted in forming the W-string); or the D-string with parameters $q_1, \ldots, q_{n-1}+1$ and $x_1, \ldots, x_{n-1}$ (if an L_{n-1} block is broken but we are not in the exceptional case). The blocks d_n^+ and d_n^- are given explicitly below.

2. We have

$$d_n^- \ldots d_1^- d_1^+ d_2^+ \ldots d_n^+ = d_n^- \widetilde{d}_{n-1}^- \widetilde{d}_{n-1}^+ d_n^+ = S_n.$$

(The $d_1^- d_1^+$ in the middle, if not both empty, must be merged to form a single L_1 or S_1 block.)

3. The W-string has the form $\widehat{w}_n \ldots \widehat{w}_1$, where each $\widehat{w}_k$ is obtained by "rearranging" that string as specified below.

To carry through the recursion, we need to allow $q_n = 1$.

5.3 Description of the d_n^+, d_n^- and $\widehat{w}_n$

Let t be the number of initial zeros in the sequence $x_{n-1}, x_{n-2}, \ldots, x_1$ (so $0 \le t \le n-1$).

5.3.1 $n = 1$

$$d_1^+ = *^{q_1 - x_1}, \qquad d_1^- = *^{x_1}, \qquad \widehat{w}_1 = *^{\max(q_1 - x_1, x_1)} *^{\min(q_1 - x_1, x_1)} .$$

5.3.2 n even

5.3.2.1 No level $n-1$ block broken

This occurs if $t = n-1$. We then have

$$d_n^+ = S_{n-1}^{x_n}, \qquad d_n^- = L_{n-1} S_{n-1}^{q_n - x_n - 1}, \qquad \widehat{w}_n = L_{n-1} S_{n-1}^{q_n - 1}.$$

5.3.2.2 An L_{n-1} is broken

This occurs when $t \neq n-1$ and $q_n = 1$ (so $x_n = 0$). In this case, d_n^+, d_n^- and $\widehat{w}_n$ are all empty.

It also occurs if $t \neq n-1$, $q_n \geq 2$, and either t is even, $x_n = 0$, when

$$d_n^+ = S_{n-1}^{q_n-1}, \qquad d_n^- \text{ is empty}, \qquad \widehat{w}_n = S_{n-1}^{q_n-1}.$$

or t is odd, $x_n = q_n - 1$ (the **exceptional case**) when

$$d_n^+ = L_{n-2}S_{n-1}^{q_n-2}, \qquad d_n^- = S_{n-2}^{q_{n-1}}, \qquad \widehat{w}_n = L_{n-1}S_{n-1}^{q_n-2}.$$

In the exceptional case, we continue with parameters $(q_1, \ldots, q_{n-1})$ and $(x_1, \ldots, x_{n-1})$, whereas in all other situations where the L_{n-1} is broken, we continue with parameters $(q_1, \ldots, q_{n-1}+1)$ and $(x_1, \ldots, x_{n-1})$.

5.3.2.3 An S_{n-1} is broken

This occurs if $t \neq n-1$, $q_n \geq 2$, and either t is even, $x_n \neq 0$, when

$$d_n^+ = S_{n-1}^{x_n-1}, \qquad d_n^- = L_{n-1}S_{n-1}^{q_n-x_n-1},$$

or t is odd, $x_n \neq q_n - 1$, when

$$d_n^+ = S_{n-1}^{x_n}, \qquad d_n^- = L_{n-1}S_{n-1}^{q_n-x_n-2}.$$

In both these cases,

$$\widehat{w}_n = L_{n-1}S_{n-1}^{q_n-2}.$$

5.3.3 $n \geq 3$, odd

5.3.3.1 No level $n-1$ block broken

This occurs if $t = n-1$. We then have

$$d_n^+ = S_{n-1}^{q_n-x_n-1}L_{n-1}, \qquad d_n^- = S_{n-1}^{x_n},$$

and

$$\widehat{w}_n = \begin{cases} S_{n-1}^{q_n-x_n-1}L_{n-1}S_{n-1}^{x_n} & \text{if } x_n \leq \frac{1}{2}q_n, \\ S_{n-1}^{x_n-1}L_{n-1}S_{n-1}^{q_n-x_n} & \text{if } \frac{1}{2}q_n \leq x_n < q_n. \end{cases}$$

(The two formulae for $\widehat{w}_n$ agree if $x_n = \frac{1}{2}q_n$.)

5.3.3.2 An L_{n-1} is broken

This occurs when $t \neq n-1$ and $q_n = 1$ (so $x_n = 0$). In this case, d_n^+, d_n^- and $\widehat{w}_n$ are all empty.

It also occurs if $t \neq n-1$, $q_n \geq 2$, and either t is even, $x_n = 0$ or t is odd, $x_n = q_n - 1$. In either case,

$$d_n^+ \text{ is empty}, \qquad d_n^- = S_{n-1}^{q_n-1}, \qquad \widehat{w}_n = S_{n-1}^{q_n-1}.$$

5.3.3.3 An S_{n-1} is broken

This occurs if $t \neq n-1$, $q_n \geq 2$, and either t is even, $x_n \neq 0$, when

$$d_n^+ = S_{n-1}^{q_n-x_n-1} L_{n-1}, \qquad d_n^- = S_{n-1}^{x_n-1},$$

$$\widehat{w}_n = S_{n-1}^{\max(q_n-x_n-1, x_n-1)} L_{n-1} S_{n-1}^{\min(q_n-x_n-1, x_n-1)},$$

or t is odd, $x_n \neq q_n - 1$, when

$$d_n^+ = S_{n-1}^{q_n-x_n-2} L_{n-1}, \qquad d_n^- = S_{n-1}^{x_n},$$

$$\widehat{w}_n = \begin{cases} S_{n-1}^{q_n-x_n-2} L_{n-1} S_{n-1}^{x_n} & \text{if } x_n \leq \frac{1}{2} q_n - 1, \\ S_{n-1}^{x_n-1} L_{n-1} S_{n-1}^{q_n-x_n-1} & \text{if } \frac{1}{2} q_n - 1 < x_n < q_n - 1. \end{cases}$$

The first step in proving these are indeed the correct descriptions is to show the D-strings agree with those obtained from Algorithm 4.10.

5.4 Reconciliation with Algorithm 4.10

Firstly, when $n = 1$, Algorithm 4.10 gives $*^{q_1-x_1}*^{x_1}$, as required.

When $t = n - 1$ (so $x_{n-1} = 0 = \ldots = x_1$), then Algorithm 4.10 converts $S_n = L_{n-1} S_{n-1}^{q_n-1}$ to $S_{n-1}^{x_n} \mid L_{n-1} S_{n-1}^{q_n-x_n-1}$ (for n even), or $S_n = S_{n-1}^{q_n-1} L_{n-1}$ to $S_{n-1}^{q_n-x_n-1} L_{n-1} \mid S_{n-1}^{x_n}$ (for n odd), where $\mid$ indicates the point at which S_n is broken. This is valid even for $x_n = 0$, or indeed $q_n = 1$.

If $q_n = 1$ then the string $S_n = L_{n-1} S_{n-1}^{q_n-1}$ (for n even) or $S_n = S_{n-1}^{q_n-1} L_{n-1}$ (for n odd) is just L_{n-1}, i.e., the S-string for parameters $q_1, \ldots, q_{n-2}, q_{n-1} + 1$. This reflects the equality of continued fractions $[0; q_1, \ldots, q_{n-1}, 1] = [0; q_1, \ldots, q_{n-1} + 1]$.

So we may assume $n > 1$, $q_n > 1$, and $t < n-1$.

Suppose that n is even. Starting from $S_n = L_{n-1}S_{n-1}^{q_n-1}$, we first move x_n copies of S_{n-1} from right to left, giving

$$S_{n-1}^{x_n}L_{n-1}S_{n-1}^{q_n-x_n-1}. \tag{5.2}$$

If $t = 0$ (so $x_{n-1} \neq 0$), we next move x_{n-1} copies of S_{n-1} from the leftmost block (S_{n-1} if $x_n > 0$ and L_{n-1} if $x_n = 0$). This gives a string of the form

$$\begin{cases} (\text{end of } S_{n-1})S_{n-1}^{x_n-1} \mid L_{n-1}S_{n-1}^{q_n-x_n-1}(\text{start of } S_{n-1}) & \text{if } x_n > 0, \\ (\text{end of } L_{n-1})S_{n-1}^{q_n-1} \mid (\text{start of } L_{n-1}) & \text{if } x_n = 0. \end{cases} \tag{5.3}$$

In particular, for $t = 0$, the L_{n-1} block is broken if and only if $x_n = 0$.

If $t = 1$ (so $x_{n-1} = 0$ and $x_{n-2} \neq 0$) the second step of the algorithm leaves the string as in (5.2) and the third step moves x_{n-2} copies of S_{n-2} from right to left, breaking the rightmost S_{n-1} block (if $x_n < q_n - 1$) or the L_{n-1} block (if $x_n = q_n - 1$). Thus we get a string of the form

$$\begin{cases} (\text{end of } S_{n-1})S_{n-1}^{x_n-1} \mid L_{n-1}S_{n-1}^{q_n-x_n-1}(\text{start of } S_{n-1}) & \text{if } x_n < q_n - 1, \\ (\text{end of } L_{n-1})S_{n-1}^{q_n-1} \mid (\text{start of } L_{n-1}) & \text{if } x_n = q_n - 1. \end{cases} \tag{5.4}$$

In particular, for $t = 1$, the L_{n-1} block is broken if and only if $x_n = q_n - 1$.

If $t = 2$, then the leftmost block in (5.2) is broken by moving x_{n-3} copies of S_{n-2}, and so on. Thus, the leftmost (respectively, rightmost) block is broken if t is even (respectively, odd). Hence, the L_{n-1} block is broken if t is even and $x_n = 0$, or t is odd and $x_n = q_n - 1$, and an S_{n-1} block is broken otherwise. Subsequent steps of the Algorithm move segments between the (end of S_{n-1}) and (start of S_{n-1}) (respectively, (end of L_{n-1}) and (start of L_{n-1})) if an S_{n-1} block (respectively, the L_{n-1} block) is broken, so that the string continues to have the same form, (5.3) or (5.4), according to the parity of t. When the algorithm terminates, the string (end of S_{n-1})(start of S_{n-1}) (respectively, (end of L_{n-1})(start of L_{n-1})) is the D-string for parameters $q_1, \ldots, q_{n-1}$ (respectively, $q_1, \ldots, q_{n-1} + 1$) and $x_1, \ldots, x_{n-1}$. This gives d_n^+ and d_n^- as stated in §5.3.2.2 and §5.3.2.3 in all cases apart from the exceptional case with t odd and $x_n = q_n - 1$.

In the exceptional case, the above discussion would give $d^+ = S_{n-1}^{q_n-1}$ and d^- empty, but we need to carry the analysis further to obtain an intelligible W-string. Looking at the string in (5.2) – obtained from the first step of the Algorithm with $x_n = q_n - 1$ – we can expand the first and last block to obtain

$$S_{n-2}^{q_{n-1}-1} L_{n-2} S_{n-1}^{q_n-2} \mid S_{n-2}^{q_{n-1}} L_{n-2}.$$

As t is odd, some part of the rightmost L_{n-2} will be moved to the left, giving a string of the form

$$(\text{end of } L_{n-2}) S_{n-2}^{q_{n-1}-1} L_{n-2} S_{n-1}^{q_n-2} \mid S_{n-2}^{q_{n-1}} (\text{start of } L_{n-2}).$$

Since $L_{n-2} S_{n-2}^{q_{n-1}-1} = S_{n-1}$, we may rewrite this as

$$(\text{end of } S_{n-1}) L_{n-2} S_{n-1}^{q_n-2} \mid S_{n-2}^{q_{n-1}} (\text{start of } S_{n-1}),$$

where (end of S_{n-1})(start of S_{n-1}) is the D-string for parameters $(q_1, \ldots, q_{n-1})$ and $(x_1, \ldots, x_{n-1})$. This gives d_n^+ and d_n^- as stated in the exceptional case.

Finally, when n is odd, we start from $S_n = S_{n-1}^{q_n-1} L_{n-1}$, and first move x_n copies of S_{n-1} from left to right, giving $S_{n-1}^{q_n-x_n-1} L_{n-1} S_{n-1}^{x_n}$. We again find that the L_{n-1} block is broken if either t is even and $x_n = 0$, or t is odd and $x_n = q_{n-1}$, and we obtain the descriptions of d_n^+ and d_n^- as in §5.3.3.2 and §5.3.3.3 by similar arguments as for n even.

Now that we have reconciled this description of the D-string with Algorithm 4.10, we aim to show we can also now describe the W-string.

5.5 Proving the description of the W-string

Let us introduce some new terminology.

- We say two strings are *equivalent* if they have the same length and give the same jump (i.e., contain the same number of level 1 blocks; we will only use this terminology for strings consisting of unbroken level 1 blocks).

- We say a string A of length k, with corresponding sequence $a(0), \ldots, a(k-1)$, is *attainable* if, for each $j < k$, there is some u with $d(j+u) - d(u) = a(j)$. Loosely speaking, an attainable string is a candidate for an initial segment of W, but better candidates may exist.

- Given a D-string (end of S_n) $|$ (start of S_n), where (end of S_n) has length λ, we say $w(j)$ is *achieved at* u if $w(j) = d(j+u) - d(u)$. Thus $w(j)$ is achieved at some $u < p - j$. Also, we will say $w(j)$ is *achieved with* $|$ if $w(j)$ is achieved for some u with $\lambda - j - 1 \leq u \leq \lambda$; this means that one of the (possibly many) segments of length j in the D-string which achieve $w(j)$ is either the final segment of (end of S_n) (ending at $|$, so $u = \lambda - j - 1$), or the initial segment of (start of S_n) (starting at $|$, so $u = \lambda$) or includes parts of both (end of S_n) and (start of S_n) (with $|$ occuring inside the string).

- We call a segment A of a string B a *proper* segment if no level 1 blocks in B are broken to form A. For example, L_1 is a proper initial segment of $S_2 = L_1 S_1^{q_2-1}$, while S_1 is an initial segment of S_2 but not a proper initial segment.

In §5.3 we have in each case split the D-string into 4 proper segments: $D = D^+ d_n^+ \mid d_n^- D^-$, where $D^+ d_n^+ =$ (end of S_n), $d_n^- D^- =$ (start of S_n), and $D^+ D^-$ is either empty (if no level $n-1$ block is broken; this includes the case $n = 1$), or $D^+ D^- = S_{n-1}$ (if a S_{n-1} block is broken, or we are in the exceptional case), or $D^+ D^- = L_{n-1}$ (if a L_{n-1} block is broken, and we are not in the exceptional case). In each case, we have also specified a string $\widehat{w}_n$ equivalent to $d_n^+ d_n^-$.

Theorem 5.6. *The W-string corresponding to D is $\widehat{w}_n W_{n-1}$, where W_{n-1} is the W-string corresponding to $D^+ \mod D^-$.*

Before we prove this statement, we turn to the following example, in order to clearly illustrate how this all works:

Example 5.7. *Let $[q_0; q_1, q_2, q_3, q_4] = [0; 5, 3, 4, 3]$ (and so $\frac{s}{p} = \frac{42}{223}$). In this case,* *by (4.2) and (4.3), we have:*

$$
\begin{aligned}
L_2 &= L_1S_1^3, \quad S_2 = L_1S_1^2 \\
L_3 &= (L_1S_1^2)^4L_1S_1^3, \quad S_3 = (L_1S_1^2)^3L_1S_1^3 \\
S_4 &= L_3S_3^2.
\end{aligned}
$$

Let's take the case when $(x_1, x_2, x_3, x_4) = (1, 0, 2, 0)$, which is the case when $h = -6$. By Algorithm 4.10, we rearrage S_4 firstly without breaking any S_3 blocks on the right. This means the L_3 block on the left gets broken when we move $x_3 = 2$ S_2 blocks right to left:

$$S_2^2L_2S_3^2S_2^2.$$

Now, there are no S_1 blocks to move, but we must break an L_1 block on the left in order to move $x_1 = 1$ lots of $*$ from left to right. This gives:

$$D = *^4S_1^2S_2L_2S_3^2S_2^2 * .$$

Note that in doing this rearrangement, we have only broken an L_3 and an L_1 block.

So now we want to find $W = \widehat{w}_4\widehat{w}_3\widehat{w}_2\widehat{w}_1$. By §5.3.2.2, $\widehat{w}_4 = S_3^2$ since $t = 0 = x_4$. By §5.3.3.1, $\widehat{w}_3 = S_3^{q_3-x_3-1}L_3S_3^{x_3} = S_3L_3S_3^2$. By §5.3.2.2, $\widehat{w}_2 = S_3^2$, since $t = 0 = x_2$. Finally, by §5.3.1, $\widehat{w}_1 = *^4*$.

Putting this all together, then, we obtain:

$$
\begin{aligned}
W &= S_3^2S_2L_2S_2^2S_1^2 *^4 * \\
&= ((L_1S_1^2)^3L_1S_1^3)^2L_1S_1^2L_1S_1^3(L_1S_1^2)^2S_1^2 *^4 *.
\end{aligned}
$$

So this is the string of the sequence of the $\{w(j)\}$, as j varies, for the case $\frac{42}{223} = [0; 5, 3, 4, 3]$, when $h = -6$.

We will now prove the sequence of W's is as described.

Proof of Theorem 5.6

Let the strings D^+, d_n^+, d_n^-, D^- have lengths α, β, γ, δ respectively, and set $\mu = \beta + \gamma$.

We argue inductively, the case $n = 1$ being clear. If $n \geq 2$ and $q_n = 1$, we can reduce to the case $n - 1$ (with q_{n-1} replaced by $q_{n-1} + 1$), so we may suppose inductively that this case has already been handled. We therefore assume $n \geq 2$ and $q_n \geq 2$.

The claim $W = \widehat{w}_n W_{n-1}$ amounts to the three assertions

Assertion 1. if $j < \gamma + \delta$ then $w(j) = \widehat{w}_n(j)$;

Assertion 2. if $\mu < p$ then $w(\mu) = 1 + w(\mu)$;

Assertion 3. if $\mu < j < p$ then $w(j) = w(\mu) + w_{n-1}(j - \mu)$.

We will prove these case by case over the next few (sub)sections. Note that the optimality properties of the strings S_m mean that S_k is a (possibly improper) initial segment of S_m, and of L_m, whenever $k \leq m$, and that $w(j) \geq d_0(j)$, where d_0 is the sequence coming from S_n.

5.5.1 n even, an S_{n-1} is broken

By §5.3.2.3 we have

$$d_n^+ \mid d_n^- = S_{n-1}^a \mid L_{n-1} S_{n-1}^b, \qquad D^+ \mid D^- = (\text{end of } S_{n-1}) \mid (\text{start of } S_{n-1})$$

with $a + b = q_n - 2$, and $\widehat{w}_n = L_{n-1} S_{n-2}^{q_n - 2}$, which is an initial segment of $S_{n-1} = L_{n-1} S_{n-2}^{q_n - 1}$.

Assertion 1.: If $j < l_{n-1} + b s_{n-1}$ then the initial segment of $d_n^- = L_{n-1} S_{n-1}^b$ gives

$$d(\alpha + \beta + j) - d(\alpha + \beta) = \widehat{w}_n(j).$$

If $l_{n-1} + (b + c - 1) s_{n-1} \leq j < l_{n-1} + (b + c) s_{n-1}$ with $1 \leq c \leq a$, then the initial segment of $S_{n-1}^c L_{n-1} S_{n-1}^b$ gives

$$d(\alpha + \beta - c s_{n-1} + j) - d(\alpha + \beta - c s_{n-1}) = \widehat{w}_n(j).$$

In both cases, we therefore have $w(j) \leq \widehat{w}_n(j) = d_0(j) \leq w(j)$, so $w(j) = \widehat{w}_n(j)$.

Assertion 2.

$$w(\mu) \leq d(\alpha + \mu) - d(\alpha) = 1 + w(\mu - 1) = d_0(\mu) \leq w(\mu).$$

Assertion 3. Let $j = \mu + k$ with $k \geq 0$. Note that S_{n-1} is both an initial segment and a final segment (possibly improper) of $S_{n-1}^a L_{n-1} S_{n-1}^b$ (even if $a = 0$ or $b = 0$). Now

$$w_{n-1}(k) = \min\{d_{n-1}(k+u) - d_{n-1}(u) : 0 \leq u < \alpha + \delta - k\},$$

where the sequence d_{n-1} comes from the string

$$D_{n-1} = (\text{end of } S_{n-1}) \mid (\text{start of } S_{n-1})$$

of length $\alpha + \delta$. We claim that, for $0 \leq u \leq \alpha + \delta - k$, we have

$$d(\mu + k + u) - d(u) = w(\mu) + d_{n-1}(k+u) - d_{n-1}(u), \tag{5.5}$$

Then, taking the minimum over u, will give $w(j) = w(\mu) + w_{n-1}(j - \mu)$, as required.

If $u \leq \alpha$ and $u + k \geq \alpha$, then (5.5) holds since the string corresponding to the left-hand side is just the string corresponding to $w(\mu) + d_{n-1}(k+u) - d_{n-1}(u)$ with $S_{n-1}^a L_{n-1} S_{n-1}^b$ inserted in the middle.

If $u + k = \alpha - \varepsilon$ with $\varepsilon > 0$, we have $d_{n-1}(u) = d(u)$ since $u < \alpha$, and $d(\alpha) - d(\alpha - \varepsilon) = d(\alpha + \mu) - d(\alpha + \mu - \varepsilon)$ because S_{n-1} is a final segment of $S_{n-1}^a L_{n-1} S_{n-1}^b$. So

$$\begin{aligned}
&d(\mu + k + u) - d(u) \\
&\quad = [d(\mu + \alpha - \varepsilon) - d(\alpha)] + [d(\alpha) - d(\alpha - \varepsilon)] + [d(k+u) - d(u)] \\
&\quad = [(d(\alpha + \mu) - d(\alpha)] + d_{n-1}(k+u) - d_{n-1}(u).
\end{aligned}$$

Hence (5.5) holds in this case. Similarly, if $u + k = \alpha + \mu = \varepsilon$ then (5.5) holds since S_{n-1} is an initial segment of $S_{n-1}^a L_{n-1} S_{n-1}^b$.

5.5.2 n even, no level $n-1$ block broken

Assertion 1 holds by the same argument as in §5.5.1. *Assertions 2* and *3* do not occur as $D^+ D^-$ is empty.

5.5.3 n even, an L_{n-1} is broken

The D-string has the form (end of L_{n-1})$S_{n-1}^{q_n-1}$ | (start of L_{n-1}). When $x_n = q_n - 1$ and t is odd, the shortest possible (start of L_{n-1}) occurs with $x_n = q_n = 1$, $x_{n-1} = 0$, $x_{n-2} = q_{n-2}$, $\ldots$, $x_2 = q_2$, $x_1 = 0$, when we have

$$(\text{start of } L_{n-1}) = S_{n-2}^{q_{n-1}} S_{n-4}^{q_{n-3}} \ldots S_2^{q_3} L_1.$$

If we replace the final L_1 in this string with S_1, we obtain

$$S_{n-2}^{q_{n-1}} S_{n-4}^{q_{n-3}} \ldots S_2^{q_3} S_1 = S_{n-2}^{q_{n-1}} S_{n-4}^{q_{n-3}} \ldots S_2^{q_3-1} L_2 = \ldots = S_{n-1}.$$

This shows that S_{n-1} is an improper initial segment of L_{n-1}, and that any (start of L_{n-1}) of length $> s_{n-1}$ occurs with $x_n = q_n - 1$ and t odd, while any (start of L_{n-1}) of length $\leq s_{n-1}$ occurs with $x_n = 0$ and t even.

We shall now deal with these two scenarios separately.

5.5.3.1 $x_n = q_n - 1$, t odd

This is the exceptional case, and we have $\mu = l_{n-1} + (q_n - 2)s_{n-1}$. Let $\mu' = (q_n - 1)s_{n-1}$, so that the D-string can be written

$$(\text{end of } L_{n-1}) S_{n-1}^{q_n-1} \mid (\text{start of } L_{n-1}),$$

where the (start of L_{n-1}) begins at position $\alpha + \mu'$, and has length $\delta' = p - \alpha - \mu' > s_{n-1}$.

Clearly W starts with the (improper) initial segment S_{n-1} of S_n, so $w(j) = d_0(j)$ for $j < s_{n-1}$. To show that W has a proper initial segment $\widehat{w}_n = L_{n-1}S_{n-1}^{q_n-2}$, we need to show that $w(j) = d_0(j)$ for $s_{n-1} \leq j \leq (q_n - 1)s_{n-1} + s_{n-2}$. Let $v_{n-1} = d_0(l_{n-1} + s_{n-1}) - d_0(l_{n-1})$ be the jump associated with S_{n-1}. Then $w(s_{n-1}) = v_{n-1} - 1 = d(\alpha + \mu' + s_{n-1}) - d(\alpha + \mu')$ since S_{n-1} is an improper initial segment of (start of L_{n-1}). From the palindrome property of S_n, we have $d(\alpha + \mu') - d(\alpha + \mu' - k) = d_0(k) + 1$ whenever $0 < k \leq \alpha + \mu'$. Hence $d(\alpha + \mu' + s_{n-1}) - d(\alpha + \mu' - k) = d_0(k) + v_{n-1}$ for such k. But since the sequence d_0 corresponds to $S_n = S_{n-2}S_{n-1}^{q_n}$, we have $d_0(k) + v_{n-1} = d_0(k + s_{n-1})$

for $s_{n-2} \leq k \leq p - s_{n-1} - 1$. As $\alpha + \mu' > p - l_{n-1}$, we conclude that $w(k+s_{n-1}) = d_0(k+s_{n-1})$ for $0 \leq k \leq p-l_{n-1}$. Thus $w(j) = d_0(j)$ for $j \leq p-s_{n-2}$. In particular, W has a proper initial segment $L_{n-1}S_{n-1}^{q_n-2}$.

Since $L_{n-1} = S_{n-2}S_{n-1}$ and (start of S_{n-1}) has a proper initial segment S_{n-2}, we may rewrite the D-string as

$$(\text{end of } S_{n-1})[S_{n-1}^{q_n-1} \mid S_{n-2}](\text{start of } S_{n-1}),$$

where the square-bracketed segment is equivalent to $L_{n-1}S_{n-1}^{q_n-2}$. Since (start of S_{n-1}) is an initial segment of S_n, it follows that the W-string begins $L_{n-1}S_{n-1}^{q_n-2}$(start of S_{n-1}), while the string W_{n-1} begins (start of S_{n-1}). Thus it only remains to show

$$d(u+k+\mu') - d(u+\mu') = d(u+k) - d(u)$$

for $u+k < \alpha$. Using the palidromic property for the two S-strings L_{n-1} and S_{n-1}, which are initial segments of D_n, we obtain $d(\alpha+\mu'-i) = d(\alpha+\mu') - 1 - i$ for $0 < i < l_{n-1}$ and $d(\alpha - i) = d(\alpha) - 1 - i$ for $0 < i \leq \alpha$. Thus $d(\alpha+\mu'+u+k) - d(\alpha+\mu'+u) = d(u+k) - d(u)$ for $0 \leq k < \alpha$. Hence $w(j) = w_{n-1}(j-\mu') + d(\alpha+\mu') - d(\alpha)$ for $j \geq \mu'$, as required.

5.5.3.2 $x_n = 0$, t even

Using $L_{n-1} = S_{n-2}S_{n-1}$, we can rewrite the D-string as

$$(\text{end of } S_{n-2})S_{n-1}^{q_n} \mid (\text{start of } S_{n-2}),$$

where (end of S_{n-2}) could be empty, so (start of S_{n-2}) could be all of S_{n-2}. As S_{n-2} is an (improper) final segment of S_{n-1}, and (start of S_{n-2}) is an (improper) initial segment of S_{n-1}, we cannot improve on S_{n-1}^r for $1 \leq r \leq q_n$ and $1 \leq q_n - 1$ as a proper initial segment of W by shifting left or right in the D-string. So we get $W = \widehat{w}_n W_{n-1}$ as required.

This concludes the cases for n even. We now look at the n odd cases.

5.5.4 n odd, an S_{n-1} is broken

We have

$$d_n^+ \mid d_n^- = S_{n-1}^a L_{n-1} \mid S_{n-1}^b, \qquad D^+ \mid D^- = (\text{end of } S_{n-1}) \mid (\text{start of } S_{n-1})$$

with $a + b = q_n - 2$. Here $S_n = S_{n-1}^{q_n-1} L_{n-1}$.

Clearly $S_{n-1}^b(\text{start of } S_{n-1})$ is an initial segment of W, and, as S_{n-2} is a (not necessarily proper) initial segment of S_{n-1} and L_{n-1}, it follows that $S_{n-1}^a L_{n-1}$ is a (not necessarily proper) initial segment of W.

We shall now deal with the cases $a \geq b$ and $a < b$ separately.

5.5.4.1 $a \geq b$

Let $a \geq b$. We claim the string $S_{n-1}^a L_{n-1}$ is a *proper* initial segment of W, i.e., $w(\beta) = 1 + w(\beta - 1)$. We have $d(\alpha + \beta) - d(\alpha) = 1 + w(\beta - 1)$, and $d(\alpha + \beta + k) - d(\alpha + k) = d(\alpha + \beta) - d(\alpha)$ if $k > 0$ since $D^- = (\text{start of } S_{n-1})$ is an initial segment of $d_n^+ = S_{n-1}^a L_{n-1}$. (This is true even if $a = 0$ since $L_{n-1} = S_{n-1}S_{n-2}$.) The same applies for $k < 0$ if $b > 0$ since then $D^+ = (\text{end of } S_{n-1})$ is a final segment of $d_n^- = S_{n-1}^b$. So suppose $b = 0$. We must compare (end of S_{n-1}) with the end of L_{n-1}. We have the expansions

$$S_{n-1} = L_1 S_1^{q_2-1} S_2^{q_3-1} L_2 S_3^{q_4-1} S_4^{q_5-1} L_4 \dots L_{n-3} S_{n-2}^{q_{n-1}-1},$$

$$L_{n-1} = S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \dots S_2^{q_3} L_1 S_1^{q_2} S_2^{q_3-1} L_2 S_3^{q_4-1} S_4^{q_5-1} L_4 \dots L_{n-3} S_{n-2}^{q_{n-1}-1}.$$

Since (end of S_{n-1}) cannot be the whole of S_{n-1}, it exactly matches the final segment of the same length in L_{n-1}. Hence we indeed have that $S_{n-1}^a L_{n-1}$ is a proper initial segment of W of length β.

Now if $\beta < j \leq \beta + \gamma$ we have

$$w(j) \leq d(\alpha + j) - d(\alpha) = d(\alpha + j) - d(\alpha + \beta) + w(\beta) = w(j - \beta) + w(\beta) \leq w(j),$$

so that $w(j) = w(\beta) + w(j - \beta)$. This shows that W has initial segment $\widehat{w}_n = S_{n-1}^a L_{n-1} S_{n-1}^b$ (this is consistent with §5.3.3.3), proving *Assertions 1* and *2*.

It remains to prove *Assertion 3*. This holds as in §5.5.1 since $D^+ =$ (end of S_{n-1}) is a final segment of $d_n^- = S_{n-1}^b$ (even when $b = 0$, as shown above) and $D^- =$ (start of S_{n-1}) is an initial segment of $d_p^- = S_{n-1}^{a+1} L_{n-1}$.

5.5.4.2 $b > a$

Now let $b > a$. Although S_{n-1}^b is an initial segment of W, we cannot always extend it to $S_{n-1}^b L_{n-1}$; if not, we must absorb the final S_{n-1} into L_{n-1}, giving an initial segment $S_{n-1}^{b-1} L_{n-1}$. In fact, we get $S_{n-1}^b L_{n-1}$ as a proper initial segment of W if t is even (with $t < n-1$), $x_n > 0$, and $S_{n-1}^{b-1} L_{n-1}$ if t is odd, $x_n < q_n - 1$. To see this, note that the D-string is (end of S_{n-1})$S_{n-1}^a L_{n-1} \mid S_{n-1}^b$(start of S_{n-1}), and that if t is even, $x_n \neq 0$ then the shortest (start of S_{n-1}) occurs when $t = 0$, $x_{n-1} = q_{n-1} - 1$, $x_{n-2} = 0$, $x_{n-3} = q_{n-3}$, $x_{n-4} = 0$, $\ldots$, $x_2 = q_2$, $x_1 = 0$, giving the D-string

$$S_1^{q_1} S_3^{q_3} \ldots S_{n-4}^{q_{n-4}} S_{n-2}^{q_{n-1}-1} S_{n-1}^a L_{n-1} \mid S_{n-1}^b S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \ldots S_2^{q_3} L_1. \tag{5.6}$$

Notice that, if in the string $D^- = S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \ldots S_2^{q_3} L_1$, we replace the final L_1 by S_1, we get the string

$$\begin{aligned} S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \ldots S_2^{q_3} S_1 &= S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \ldots S_2^{q_3-1} L_2 \\ &= S_{n-3}^{q_{n-2}} S_{n-5}^{q_{n-4}} \ldots S_4^{q_5} S_3 \\ &= \ldots \\ &= S_{n-2}. \end{aligned}$$

Thus any D-string of the form (5.6), for which D^- has length $\delta \leq s_{n-2}$, arises with t odd, $x_n < q_n - 1$, and any such D-string with $\delta > s_{n-2}$ arises with t even, $x_n > 0$. Moreover, the initial segment of S_{n-1} of length s_{n-2} (ending in the last position of the L_1) gives a smaller jump than an S_{n-2}, so

$$d_0(s_{n-2}) = d(\alpha + \beta) - d(\alpha + \beta - s_{n-2}) - 1. \tag{5.7}$$

We will now discuss the cases for t odd and even separately, showing $W = \widehat{w}_n W_{n-1}$ in each case. First, we need the following Proposition.

Proposition 5.5.5.

$$w(bs_{n-1}+s_{n-2}) = \begin{cases} d_0(bs_{n-1}+s_{n-2}) & \text{if } t \text{ is odd;} \\ d_0(bs_{n-1}+s_{n-2})-1 & \text{if } t \text{ is even.} \end{cases}$$

Proof. If t is even, so $\delta > s_{n-2}$, we have

$$\begin{aligned} & d(\alpha+\beta+bs_{n-1}+s_{n-2}) - d(\alpha+\beta) \\ = \;& [d(\alpha+\beta+bs_{n-1}+s_{n-2}) - d(\alpha+\beta+bs_{n-1})] + [d(\alpha+\beta+\gamma) - d(\alpha+\beta)] \\ = \;& d_0(s_{n-2}) + d_0(bs_{n-1}) \\ \leq \;& d_0(s_{n-2}+bs_{n-1}) \\ \leq \;& w(s_{n-2}+bs_{n-1}), \end{aligned}$$

so we have equality throughout.

Now let t be odd, so $\delta \leq s_{n-2}$. The D-string is then

$$(\text{end of } S_{n-1})S_{n-1}^{a+1}S_{n-2} \mid S_{n-1}^{b}(\text{start of } S_{n-2}),$$

where "(start of S_{n-2})" could in fact be the whole of S_{n-2}. The segment $S_{n-2}S_{n-1}^{b}$ realises a jump $d_0(s_{n-2}+bs_{n-1})+1$. We cannot improve on this by shifting the segment right or left, since $D^- =$ (start of S_{n-2}) is an initial segment, and (end of S_{n-2})S_{n-1}^{a+1} a final segment; if $b = a+1$ this follows from the fact already noted that (end of S_{n-1}), which cannot be a complete S_{n-1}, is a final segment of L_{n-1}. $\square$

Recall we are still in the n odd, S_{n-1} broken, $b > a$ case. We deal with t odd and even separately.

t **odd:**

Here $w(bs_{n-1}+s_{n-2})$ is achieved at $\alpha+\beta-l_{n-1}$ by the segment $L_{n-1}S_{n-1}^{b-1} = S_{n-1}S_{n-2}S_{n-1}^{b-1}$. Arguing as in §5.5.1, we see that W begins $\widehat{w}_n = S_{n-1}^{b-1}L_{n-1}S_{n-1}^{a+1}$. As this begins with $D^- =$ (start of S_{n-1}) and ends with $D^+ =$ (end of S_{n-1}), we can argue as before to get $W = \widehat{w}_n W_{n-1}$.

t **even:**

We know $w(j) = d_0(j)$ for $j \leq bs_{n-1} + s_{n-2}$. Our D-string has the form (end of S_{n-1})$S_{n-1}^a L_{n-1} \mid S_{n-1}^b$(start of S_{n-1}), where (start of S_{n-1}) has S_{n-2} as an improper segment. Thus, removing the last bs_{n-1} elements in the string, we are left with (end of S_{n-1})$S_{n-1}^a L_{n-1} \mid$ (start of S_{n-1}) with the same "(start of S_{n-1})", starting at position $\alpha + \beta$. Thus the segment $L_{n-1} S_{n-1}^b$(start of S_{n-1}) starting at position $\beta - l_{n-1}$ has an *improper* initial segment $L_{n-1} S_{n-2} = L_{n-2} S_{n-2}^{q_{n-1}+1}$ of length $l_{n-1} + s_{n-2}$. Now this string is an S-string (it is the "S_{n-1}" with q_{n-1} replaced by $q_{n-1} + 2$), so it has the palindromic property. Writing d' for the sequence giving this string, we therefore have

$$d(\alpha + \beta + s_{n-2} - k) = d(\alpha + \beta + s_{n-2}) - d'(k) \text{ for } 0 \leq k < l_{n-1} + s_{n-2}.$$

We then have

$$d(\alpha + \beta + \gamma + s_{n-2}) - d(\alpha + \beta + s_{n-2} - k) = bw(s_{n-1}) + d'(k).$$

But $d'(k) = w(k)$ for $k < l_{n-1}$. This shows that W has $S_{n-1}^b L_{n-1}$ as an initial segment, and it will be a *proper* initial segment provided that there is no j with

$$d(bs_{n-1} + l_{n-1} + u) - d(u) < d(\alpha + \beta + \gamma + s_{n-2}) - d(\alpha + \beta + s_{n-2} - l_{n-1}).$$

But the jump on the right is achieved by the bracketed segment $[L_{n-1} S_{n-1}^b]$ when we write the D-string as (end of S_{n-1})$S_{n-1}^a [L_{n-1} S_{n-1}^b]$(start of S_{n-1}). We cannot improve on this jump by shifting left, since (end of S_{n-1})S_{n-1}^a is a final segment of $[S_{n-2} S_{n-1}^{b+1}]$ (as $b > a$), or by shifting right as (start of S_{n-1}) is an initial segment of $L_{n-1} = S_{n-1} S_{n-2}$. This shows that W has a proper initial segment $S_{n-1}^b L_{n-1}$. Since $w(u) + w(v) \leq w(u + v)$, it then follows that W has proper initial segment $\widehat{w}_n = S_{n-1}^b L_{n-1} S_{n-1}^a$. As (start of $S_n - 1$) is an initial segment of this, and (end of S_{n-1}) a final segment (even if $a = 0$, since it has length $< l_{n-1} - s_{n-2} = s_{n-1}$), it follows as before that the W-string is $\widehat{w}_n W_{n-1}$.

5.5.6 n odd, no level $n - 1$ block is broken

This follows by the same argument as in the previous case (with t odd), where again $a = q_n - x_n - 1$ but now $b = x_n$.

5.5.7 n odd, an L_{n-1} is broken

Here the D-string is (end of L_{n-1})$S_{n-1}^{q_n-1}$(start of L_{n-1}), so the W-string starts with the initial segment $S_{n-1}^{q_n-1}$(start of L_{n-1}) of S_n.

It remains to show that if $j = \mu + k$ with $k \geq \delta$ then $w(j) = bw(s_{n-1}) + w_{n-1}(k)$. Now since both S_{n-1} and L_{n-1} are S-strings, so satisfy the palindromic property, and S_{n-1} is a proper initial segment of L_{n-1}, we have

$$d(\alpha + \mu - i) = d(\alpha + \mu) - 1 - d_0(k)$$

and

$$d(\alpha - i) = d(\alpha) - 1 - d_0(k)$$

for $1 \leq i \leq s_{n-1}$. Thus

$$d(\alpha) - d(\alpha - i) = d(\alpha + \mu) - d(\alpha + \mu - i)$$

for such i. Thus if $\alpha - s_{n-1} < k + u < \alpha$ then $d(k+u) - d(u) = d(k+u+\mu) - d(u+\mu)$. We can complete the argument as in §5.5.1 if we can show that $w(k)$ is attained for u with $u+k \geq \alpha - s_{n-1}$. But if $u+k < \alpha - s_{n-1}$ then, using the palindrome property again, $d(u+k) - d(u) = d(\alpha - u) - d(\alpha - u - k)$ with $\alpha - u \geq s_{n-1} > \alpha - s_{n-1}$ as $\alpha < l_{n-1} < 2s_{n-1}$. Hence if $w_{n-1}(k)$ is achieved at $u + k < s_{n-2} - k$ it is also acheived at $v = \alpha - u - k$ with $v + k > s_{n-2}$.

This exhausts all cases and concludes the proof. □

Now that we have the D and W-strings for general n, we may examine the general pattern of $\mathcal{D}$ and $\mathcal{E}$. These patterns turn out to be more difficult to obtain when some of the $x_i = 0$, so we begin by discussing general n case, but with the restriction that $x_i \neq 0$, for all i, before turning to the $n = 1$, $n = 2$ and $n = 3$ cases with no restrictions.

5.6 Finding $\mathcal{E}$ and $\mathcal{D}$

Recall $\{0\} \in \mathcal{D}$ and $\{0, 1\} \in \mathcal{E}$ by definition. The first thing we can do is give criteria to pick out certain elements of $\mathcal{E}$ and $\mathcal{D}$ - ones which make no assumptions on the x_i:

Lemma 5.8. *Let $q \geq 2$ and suppose that the W-string coincides with some D-string up to position q. Then $q \in \mathcal{E}$ if and only if the first q positions of the W-string form an S-string.*

Proof. If $w(q-1) = w(q)$ then neither condition is satisfied. So suppose $w(q-1) = w(q) - 1$. Set $t = w(q)$. Then, by Corollary 5.3(i), $q \in \mathcal{E}$ if and only if $w(i) + w(q-i) = t - 1$ whenever $0 < i < q$, and by Proposition 5.5, this occurs precisely when the first q positions in the W-string form an S-string. □

Lemma 5.9. *Let $d(q) > d(q-1)$, and suppose there is some $Q > q$ such that the first Q positions of the W-string form an S-string which is an initial segment of the string S_n for our parameters p, s. Then $q \in \mathcal{D}$ if and only if the first q positions in the D-string match the last q positions of this S-string, that is*

$$d(q-i) = w(Q-i) + d(q) - w(Q) \text{ for } 0 < i \leq q. \tag{5.8}$$

Proof. By Proposition 5.5 (with $h' = s$), the assumption on the W-string means that

$$w(i) + w(Q-i) = w(Q) - 1 \text{ for } 0 < i < Q.$$

If $q \in \mathcal{D}$ then $d(q) = w(q) + 1$ by Corollary 5.3(ii). On the other hand, (5.8) for $i = q$ is equivalent to $d(q) = w(Q) - w(Q-q)$, which means $d(q) = w(q) + 1$, since $q < Q$. Thus we may assume these equivalent conditions hold. Then from Corollary 5.3(ii) we have

$$\begin{aligned} q \in \mathcal{D} &\Leftrightarrow w(i) + d(q-i) = w(q) \quad \text{for } 0 < i \leq q \\ &\Leftrightarrow w(Q) - w(Q-i) - 1 + d(q-i) = w(q) \quad \text{for } 0 < i \leq q \\ &\Leftrightarrow d(q-i) = w(Q-i) + d(q) - w(Q) \quad \text{for } 0 < i \leq q. \end{aligned}$$

□

Note that none of this depends on any hypothesis of the x_i.

Proposition 5.10. *Let $n \geq 2$. The first q positions in S_n form an S-string for the following values of q:*

$$q = is_{2k-1} + s_{k-2} \quad \text{for } 2 \leq 2k \leq n, 1 \leq i \leq q_{2k},$$

except that if n is even, the value for $2k = n$, $i = q_n$ must be omitted.

Proof. Let d_0 be the sequence giving the string S_n. The first time we get an S-string is when $q = q_1 + 1 = s_1 + s_0$, which is the first L_1-block; this is also S_2 for the parameters $q_1' = q_1$ and $q_2' = 1$. Each of the initial segments L, LS, $\ldots$, $LS^{q_2-1} = S_2$ is an S-string (and there are no others up to this point). This gives $q = is_1 + s_0$ for $1 \le i \le q_2$. Once we have S_2, we do not get another S-string until $S_2^{q_3} L_2 = L_3$. We then get S-strings L_3, L_3S_3, $\ldots$, $L_3S_3^{q_4-1} = S_4$, giving $q = is_s + s_2$ for $1 \le i \le q_4$. We continue in this way, getting q_{2k} strings L_{2k-1}, $L_{2k-1}S_{2k-1}$, $\ldots$, $L_{2k_1}S_{2k-1}^{q_{2k}-1} = S_{2k}$ for each even index $2k \le n$, but if $n = 2k$ we must omit the final string S_{2k} of length p as we are only counting values $q < p$. $\square$

Note that when n is odd, the last S-string we get is S_{n-1}.

Corollary 5.11. *In the cases where $W = S_n$ (i.e., when all the $x_i = 0$) with $n \ge 2$, we have*

$$|\mathcal{E}| = \begin{cases} 1 + \sum_{i \text{ even}} q_i & \text{if } n \text{ is even;} \\ 2 + \sum_{i \text{ even}} q_i & \text{if } n \text{ is odd.} \end{cases}$$

5.7 Obtaining (the first part of) the set $\mathcal{E}$ in general

For $n \ge 2$, we list the initial segments of S_n of length $\ge q_1 + 1$ which occur as an S_m for some parameters.

The first of these are $L = L_1$, LS, $\ldots$, $LS^{q_2-1} = S_2$, since LS^i is the S_2 string with q_2 replaced by $i + 1$. Hence

$$\mathcal{E} \cap [0, s_2] = \{0, 1, is_1 + 1 \text{ for } 1 \le i \le q_2\}.$$

As we extend the initial part of S_n from S_2 to $S_2^{q_3} L_2 = L_3$ we do not get any further complete S_m-strings (for any parameters) until we reach S_3 itself. (This is because the L_2 comes at the end of an S_3 string, whereas $L = L_1$ comes at the start of an L_2 string.) In the same way, the strings

$$L_3,\ L_3S_3,\ \ldots,\ L_3S_3^{q^4-1} = S_4,\ L_5,\ L_5S_5,\ \ldots$$

each contribute to $\mathcal{E}$. We can continue in this way for as long as the initial part of the W-string coincides with the initial part of an S_m-string for some parameters. The elements of $\mathcal{E}$ up to this point are therefore

$$0, 1, is_j + s_{j-1} \text{ for } j \text{ odd, } 0 \leq i \leq q_j.$$

The same analysis holds for a string L_n (for some n), since this is just an S_n with q_n replaced by $q_n + 1$.

5.8 The Case $x_i \neq 0$

Assume that $x_i \neq 0$ for all i. This implies $0 < x_i < q_i$ for all i, so, in particular, $q_i \geq 2$ for all i.

5.8.1 $\mathcal{E}$ for general n, with all $x_i \neq 0$

Proposition 5.12. *Let none of the x_i be zero. For even n, the set $\mathcal{E}$ can be described as:*

$$\begin{aligned}
\mathcal{E} = \{&0, 1, \\
&is_1 + s_0 \quad \text{for } 1 \leq i \leq q_2, \\
&is_3 + s_2 \quad \text{for } 1 \leq i \leq q_4, \\
&\quad\vdots \\
&is_{n-1} + s_{n-2} \quad \text{for } 1 \leq i \leq q_n - 1 \\
&p - \min(q_{2k-1} - x_{2k-1}, x_{2k-1}) \cdot s_{2k-2} \quad \text{for } k = 1, \ldots, \frac{n}{2}\}.
\end{aligned}$$

Hence, for even n,

$$|\mathcal{E}| = 1 + \frac{n}{2} + \sum_{i \text{ even}} q_i. \tag{5.9}$$

For odd n:

$$\begin{aligned}
\mathcal{E} = \{&0, 1,\\
&is_1 + s_0 \quad \text{for } 1 \le i \le q_2,\\
&is_3 + s_2 \quad \text{for } 1 \le i \le q_4,\\
&\quad\vdots\\
&is_{n-2} + s_{n-3} \quad \text{for } 1 \le i \le q_{n-1}\\
&p - \min(q_{2k-1} - x_{2k-1}, x_{2k-1}) \cdot s_{2k-2} \quad \text{for } k = 1, \dots, \frac{n+1}{2}\}.
\end{aligned}$$

Thus,

$$|\mathcal{E}| = 2 + \frac{n+1}{2} + \sum_{i \text{ even}} q_i. \tag{5.10}$$

Proof. If n is even, we have $w_n = \widehat{w}_n\widehat{w}_{n-1}\dots\widehat{w}_1$, where $\widehat{w}_n = L_{n-1}S_{n-1}^{q_n-2}$ is S_n with the final S_{n-1} missing. By Lemma 5.8, $\mathcal{E}$ contains the $1 + \sum_{i \text{ even}} q_i$ elements listed in Proposition 5.10, together with any contributions from the $\widehat{w}_i$ with $i < n$. We will show later that there is one further element in $\mathcal{E}$ for each odd i.

If $n \ge 3$ is odd, $\widehat{w}_n$ starts with S_{n-1}. (Since $L_{n-1} = S_{n-1}S_{n-2}$, this is true even in the cases $q_n = 2$, $x_n = 1$ or $q_n = 3$, $x_n = 2$ when it actually begins with L_{n-1}.) Thus $\mathcal{E}$ contains the $2+\sum_{i \text{ even}} q_i$ elements listed in Proposition 5.10. It also contains the length of the string $S_{n-1}^M L_{n-1}$ with $M = \max(q_n - x_n - 1, x_n - 1)$ (since this string is an S_n for $q_n' = M + 1$) and any contributions from the $\widehat{w}_i$ with $i < n$. Again, we will show there is one extra contribution from each odd $i < n$. So now suppose we have already described the part of $\mathcal{E}$ coming from $\widehat{w}_N \dots \widehat{w}_{k+1}$. We need to see if there is any contribution from $\widehat{w}_k$. Let $\widehat{w}_k$ begin at position α. If k is even then $\widehat{w}_k$ is already an initial segment of the W-string, so $w(j + \alpha) = w(\alpha) + w(j)$ for all relevant j. This means we get no further contributions to $\mathcal{E}$. Next suppose k is odd with $k \ge 3$, so $\widehat{w}_k = S_{k-1}^M L_{k-1} S_{k-1}^m$ where $m = \min(x_k - 1, q_k - x_k - 1) = 0$. Let β be the first position after the end of the L_{k-1}. This is the only possible contribution to $\mathcal{E}$ from $\widehat{w}_k$ since $S_{k-1}^M L_{k-1}$ and S_{k-1}^m are initial segments of W (although the first is improper). We must show that β is indeed an element of $\mathcal{E}$.

If $m > 0$ (that is, $1 < x_k < q_k - 1$) then we may change x_k to reduce m by one; this does not affect any part of the W-string before position β, but replaces $w(\beta)$

by $w(\beta)-1$. As this is still a valid W-string (with different $x_i > 0$), we have

$$\max\{w(u)+w(v) \;:\; w+v=\beta\} \leq w(\beta)-1,$$

so that $\beta \in \mathcal{E}$. When $m=0$, we can apply the same argument since $\widehat{w}_n \ldots \widehat{w}_{k+1} S_k$ is still a valid W-string.

The same argument also works for the special case $k=1$, where we can reduce $*^{\min(q_1-x_1,x_1)}$ and use that $\widehat{w}_n \ldots \widehat{w}_2 S_1$ is a valid W-string. So in all cases when k is odd, $\beta \in \mathcal{E}$.

$\square$

5.8.2 $\mathcal{D}$ for general n with all $x_i \neq 0$

Proposition 5.13. *Let none of the x_i be zero. For even n, the set $\mathcal{D}$ can be described as:*

$$\begin{aligned}
\mathcal{D} = \{&0,\\
&is_1 - x_1 s_0 \quad \text{for } 1 \leq i \leq x_2,\\
&is_3 - x_3 s_2 - x_1 s_0 \quad \text{for } 1 \leq i \leq x_4,\\
&\quad\vdots\\
&is_{n-1} - x_{n-1}s_{n-2} + x_{n-2}s_{n-3} - \ldots + x_2 s_1 - x_1 s_0 \quad \text{for } 1 \leq i \leq x_n\}.
\end{aligned}$$

Thus, for even n,

$$|\mathcal{D}| = 1 + \sum_{\substack{i \leq n \\ i \text{ even}}} x_i. \tag{5.11}$$

For odd n, we have the following:

For $x_n \leq \frac{1}{2}q_n$, $\mathcal{D}$ is the same as the even case, i.e., the x_i with i even give rise to the elements in $\mathcal{D}$.

For $x_n > \frac{1}{2}q_n$, $\mathcal{D}$ is the same as the even case, but with one extra element, μ, at the end, where,

$$\mu = s_n - x_n s_{n-1} + x_{n-1}s_{n-2} - x_{n-2}s_{n-3} + \ldots + x_2 s_1 - x_1 s_0.$$

Hence, for odd n:

$$|\mathcal{D}| = \begin{cases} 1 + \sum_{i \text{ even}} x_i & \text{for } x_n \leq \frac{1}{2}q_n \\ 2 + \sum_{i \text{ even}} x_i & \text{for } x_n > \frac{1}{2}q_n. \end{cases} \tag{5.12}$$

Proof. First let n be even. Note that S_n ends in S_k for $k < n$ odd, and in L_k for $k < n$ even. Since W starts with the S-string $L_{n-1}S_{n-1}^{q_n-2}$, which is an initial segment of S_n, we may take Q in Lemma 5.9 to be $p - s_n - 1$. The first initial segment of D matching the end of $L_{n-1}S_{n-1}^{q_n-2}$ is $*^{q_1-x_1}$, which is the end of an S_1. Each of the segments

$$*^{q_1-x_1}S_1, \quad *^{q_1-x_1}S_1^2, \quad \ldots, \quad *^{q_1-x_1}S_1^{x_2-1}$$

is the end of an L_2, giving x_2 elements in $\mathcal{D}$ so far. Adding on $d_3^+ = S_2^{q_3-x_3-1}L_2$, we don't get any further cases until we have included the L_2, so we have the end of an S_3. The strings

$$d_1^+d_2^+d_3^+, \quad d_1^+d_2^+d_3^+S_3, \quad \ldots, \quad d_1^+d_2^+d_3^+S_3^{x_4-1} = d_1^+d_2^+d_3^+d_4^+$$

are each the end of an S_4, giving x_4 more elements contained in $\mathcal{D}$. We continue in this way until we have $x_2 + x_4 + \cdots + x_n$ elements of $\mathcal{D}$. The last of these brings us to the end of $d_1^+ \ldots d_n^+$. This has length $< Q$ since d_n^- contains an L_{n-1}. Adding in the L_{n-1} cannot give a further element of $\mathcal{D}$. (Note that, for n even, L_{n-1} does not start with S_{n-1}), and Lemma 5.9 allows no further elements $< Q$ in $\mathcal{D}$.

Since $0 \in \mathcal{D}$, this gives us $1 + \sum_{i \text{ even}} x_i$ elements of $\mathcal{D}$ which are less than Q. We then need to show there are no elements $\geq Q$; Lemma 5.9 does not apply here. We will do this, together with the odd case, at the end of the proof.

Now let n be odd. First observe that for n odd, L_{n-1} is an initial segment of S_{n-1}^2 (or of $S_{n-1}L_{n-1} = S_{n-1}^2 S_{n-2}$), but not a "proper one": indeed, replacing the final L_1 in L_{n-1} with an S_1 gives an initial segment of S_{n-1}^2 consisting of complete S_1 and L_1 blocks. We can see this by induction: $L_2 = L_1S_1^{q_2-1}S_1$ while $S_2^2 = L_1S_1^{q_2-1}L_1\ldots$; and $L_{2k} = L_{2k-1}S_{2k-1}^{q_{2k}-1}S_{2k-2}^{q_{2k-1}-1}L_{2k-2}$ while $S_{2k}^2 = L_{2k-1}S_{2k-1}^{q_{2k}-1}S_{2k-2}^{q_{2k-1}-1}S_{2k-2}\ldots$. This means that the string W of the form $S_{n-1}^M L_{n-1} S_{n-1}^m \ldots$ (with $M < q_n - 1$) first differs from $S_n = S_{n-1}^{q_n-1}L_{n-1}$ at the first position in S_{n-1}^m. This occurs at position

$Q = Ms_{n-1} + l_{n-1}$ in the W-string, so the first Q characters of the W-string form an S-string, and this is an initial segment of S_n (although not a proper one).

Applying Lemma 5.9 to this initial segment, we get the same $1 + \sum_{i \text{ even}} x_i$ elements of $\mathcal{D}$ as for even n; these are the only ones less than Q. Now

$$D = d_1^+ \dots d_{n-1}^+ S_{n-1}^{q_n-1-x_n} L_{n-1} S_{n-1}^{x_n-1} d_{n-1}^- \dots d_1^-.$$

Let $\alpha < s_{n-1}$ be the length of the initial part $d_1^+ \dots d_{n-1}^+$. If $x_n \leq \frac{1}{2}q_n$, we have

$$W = S_{n-1}^{q_n-1-x_n} L_{n-1} S_{n-1}^{x_n-1} \dots .$$

The first part of W coincides with the middle part of D, so that for $0 < j < (q_n - 2)s_{n-1} + l_{n-1}$, we have $d(\alpha) + w(j) = d(\alpha + j)$, and so $\alpha + j \notin \mathcal{D}$. This shows that there are no further elements in $\mathcal{D}$, except possibly some coming from the "tail" $d_{n-1}^- \dots d_1^-$ (and we will show there are none of these at the end of the proof). Note that in particular $\alpha + Q \notin \mathcal{D}$. (Lemma 5.9 does not apply here as we have gone "too far" along the D-string.)

On the other hand, if $x_n > \frac{1}{2}(q_n + 1)$, then

$$W = S_{n-1}^{x_n-2} L_{n-1} S_{n-1}^{q_n-x_n} \dots$$

with $x_n - 2 > q_n - x_n - 1$. We can apply Lemma 5.9 to the first position in D after the end of the L_{n-1}, namely to $q = \alpha + (q_n - x_n - 1)s_{n-1} + l_{n-1} < Q$. The part of the D-string up to this point is the end of the S-string given by the first Q characters of W, so $q \in \mathcal{D}$. Thus, in this case, we get one extra element in $\mathcal{D}$.

We now show there are no further elements in the "tail", treating even and odd n together. Note that D has the form

$$(\text{end of } S_{n-1}) d_n^+ d_n^- (\text{start of } S_{n-1}),$$

whereas W begins with S_{n-1} in all cases (although this need not be a proper initial segment). So if α is the position of the beginning of (start of S_{n-1}) in D then $d(\alpha + j) = d(\alpha) + w(j)$ for any $j < p - \alpha$. $\square$

In this chapter, we obtained the pattern of the W-strings in general, then we obtained the elements and cardinality of $\mathcal{D}$ and $\mathcal{E}$ for general n when none of the co-ordinates were zero, and partial results for when some of them are. In the next chapter, we look explicitly at the patterns of D and W, and the shape of $\mathcal{D}$ and $\mathcal{E}$, for all values of h in the cases when $n = 1$, $n = 2$ and $n = 3$.

Chapter 6

Without Restriction: The Cases $n = 1, 2, 3$

Now that we have obtained the general shape of $\mathcal{E}$ and $\mathcal{D}$ with the restriction that none of the x_i be zero, we state explicitly what the sets look like without these restrictions, for the cases $n = 1, 2$ and 3. We begin by conjecturing some results which can be easily seen to agree with the cases $n = 1, 2, 3$.

6.1 Conjectures for $|\mathcal{D}|$

Conjecture 6.1. *Let $n = 2k + 1$ be odd. For each $1 \leq j \leq k$ with $x_{2j} = 0$, and $x_{2j-1} \neq 0$, we add $2(k + 1 - j)$ to (5.12).*

Conjecture 6.2. *Let $n = 2k$ be even. For each $1 \leq j \leq k$, if $x_{2j} = 0$ and $x_{2j-1} > 1$, we add $2k - 2j + 1$ to (5.11).*

6.2 Conjecture for $\mathcal{E}$

Conjecture 6.3. *If, for i odd, any $x_i = 0$, then the corresponding $p - \min(q_i - x_i, x_i) \cdot s_{i-1}$ term does not appear in $\mathcal{E}$.*

6.3 The $n = 1$ case

Corollary 6.4. *For $n = 1$, we have:*

$$|\mathcal{D}| = \begin{cases} 1 & \text{if } x_1 \leq \frac{1}{2}q_1 \\ 2 & \text{otherwise;} \end{cases}$$

$$|E| = 3.$$

Proof. By Propositions 5.12 and 5.13 we have

$$\mathcal{D} = \begin{cases} \{0\} & \text{if } x_1 \leq \frac{1}{2}q_1 \\ \{0, p - x_1\} & \text{otherwise,} \end{cases}$$

and $|\mathcal{E}| = \{0, 1, p - \min(q_1 - x_1, x_1)\}$.

□

6.4 The $n = 2$ case

Corollary 6.5. *For $n = 2$, we have three main cases to consider.*

Case 1: For $x_1 = 0$ and $0 \leq x_2 < q_2$:

$$|\mathcal{D}| = x_2 + 1, \qquad |\mathcal{E}| = q_2 + 1.$$

Case 2: For $x_1 \neq 0, x_2 = 0$:

(a) For $x_1 = 1$, $|\mathcal{D}| = 1$, and $|\mathcal{E}| = 3$.

(b) For $x_1 = q_1$, $|\mathcal{D}| = 2$, and $|\mathcal{E}| = 3$.

(c) For $1 < x_1 < q_1$, $|\mathcal{D}| = 2$ and $|\mathcal{E}| = 4$.

Case 3: For $x_1 \neq 0, x_2 \neq 0$:

$$|\mathcal{D}| = x_2 + 1, \qquad |\mathcal{E}| = q_2 + 2.$$

Proof. Propositions 5.12 and 5.13 cover the cases when $x_2 \neq 0$: *Case 1:* For $x_1 = 0$ and $0 \leq x_2 < q_2$, clearly

$$\mathcal{D} = \{0, q_1, 2q_1, \ldots, x_2 q_1\},$$

and

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, (q_2 - 1)q_1 + 1\}.$$

Case 3: When $x_1 x_2 \neq 0$, we have:

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots (q_2 - 1)q_1 + 1, p - \min(q_1 - x_1, x_1)\},$$

and

$$\mathcal{D} = \{0, q_1 - x_1, 2q_1 - x_1, \ldots, x_2 q_1 - x_1\}.$$

Case 2: When $x_2 = 0$, we need to look a little more carefully. (a) Firstly let $x_1 = 1$. Then

$$d_2 = S_1^{q_2} * = w_2.$$

Since d_2 and w_2 are equivalent, $\mathcal{D}$ can only contain one element, namely $\mathcal{D} = \{0\}$. We claim $\mathcal{E} = \{0, 1, q_1\}$. Clearly $0, 1, q_1 \in \mathcal{E}$. We need to show these are its only elements. The other candidates are $2q_1, 3q_1, \ldots, q_2 q_1$. For $2 \leq a \leq q_2$, we have $w(aq_1) = a$. Clearly $2q_1 \notin \mathcal{E}$ since we can choose $\alpha = \beta = q_1$ and $w(\alpha) = w(\beta) = 1$ in that case, thus $\alpha + \beta = 2q_1$ and $w(\alpha) + w(\beta) = 2$. For $3 \leq a \leq q_2$, pick $\alpha = q_1$ and $\beta = (a - 1)q_1$ so that $\alpha + \beta = aq_1$ and $w(\alpha) = 1$, $w((a - 1)q_1) = a - 1$, i.e. $w(\alpha) + w(\beta) = a$. Thus

$$\mathcal{E} = \{0, 1, q_1\}.$$

(b) Now let $x_1 = q_1$. Then

$$d_2 = * S_1^{q_2}$$

and

$$w_2 = S_1^{q_2} * .$$

Since this w_2 is equivalent to case (a), above, clearly $\mathcal{E} = \{0, 1, q_1\}$ here also. We claim $\mathcal{D} = \{0, 1\}$. Clearly these are both elements of $\mathcal{D}$, so we need only examine the other candidates which are: $q_1 + 1, 2q_1 + 1, \ldots, (q_2 - 1)q_1 + 1$. For $1 \leq a \leq q_2 - 1$,

$aq_1 + 1 \notin \mathcal{D}$ since we can pick $\alpha = 1$ and $\beta = aq_1$ so that $d(1) = 1$ and $w(aq_1) = a$, whence $d(1) + w(aq_1) = d(aq_1 + 1) = a + 1$. Thus

$$\mathcal{D} = \{0, 1\}.$$

(c) Let $x \neq \{0, 1, q_1\}$, and let $x_2 = 0$. Then

$$d_2 = *^{q_1 - x_1 + 1} S_1^{q_2 - 1} *^{x_1}$$

and

$$w_2 = S_1^{q_2 - 1} *^{\max(q_1 - x_1 + 1, x_1)} *^{\min(q_1 - x_1 + 1, x_1)}.$$

We claim $\mathcal{E} = \{0, 1, q_1, q_1 q_2 - \min(q_1 - x_1, x_1 - 1)\}$. Clearly $0, 1, q_1 \in \mathcal{E}$. Other candidates are: $2q_1, \ldots, (q_2 - 1)q_1, p - \min(q_1 - x_1 + 1, x_1)$. By the same reasoning as in case (a) - where our W sequence also began with lots of S_1's in a row - we have $2q_1, \ldots, (q_2 - 1)q_1 \notin \mathcal{E}$.

Next we note $w(p - \min(q_1 - x_1 + 1, x_1)) = q_2$ (since the w_2 sequence has q_2 blocks before the $*^{\min(q_1 - x_1 + 1, x_1)}$ block, and we start numbering from zero). We claim there do not exist $\alpha, \beta > 0$ such that $\alpha + \beta = p - \min(q_1 - x_1 + 1, x_1)$ and $w(\alpha) + w(\beta) = q_2$. If both α and β are in any of the S_1 blocks (not necessarily the same one), or if one of them is in the $*^{\max(q_1 + 1 - x_1, x_1)}$ block, we can let $w(\alpha) = r$, $w(\beta) = s$ and then $\alpha \geq rq_1$ and $\beta \geq sq_1$. So if $w(\alpha) + w(\beta) = r + s = q_2$, then $\alpha + \beta \geq (r + s)q_1 = q_2 q_1 \geq q_2$ with equality only if $q_1 = 1$. But if this is the case then since $x_1 \leq q_1$ we will have $x_1 \leq 1$ and since we have already dealt with these cases separately (in Case 1 and Case 2(a)) then we are done.

Now we claim $\mathcal{D} = \{0, q_1 - x_1 + 1\}$. The candidates are $q_1 - x_1 + 1, 2q_1 - x_1 + 1, \ldots, q_2 q_1 - x_1 + 1$. Clearly $0, q_1 - x_1 + 1 \in \mathcal{D}$ since $|S_1| \geq | *^{q_1 + 1 - x_1} |$ as $x_1 > 1$. So we need to show these other candidates are not elements of $\mathcal{D}$. We have

$$d(aq_1 - x_1 + 1) = a \quad \text{for } 1 \leq a \leq q_2$$

and

$$w(aq_1 - x_1 + 1) = a - 1 \quad \text{for } 1 \leq a \leq q_2,$$

unless $\min(q_1 + 1 - x_1, x_1) = x_1$ in which case the latter equation is valid for $1 \leq a \leq q_2 - 1$. We need to show there exists $\alpha, \beta > 0$ such that $\alpha + \beta = aq_1 - x_1 + 1$ and $d(\alpha) + w(\beta) = d(aq_1 - x_1 + 1) = a$, for $2 \leq a \leq q_2$. If we let $\alpha = (a-1)q_1 - x_1 + 1$ then $d(\alpha) = a - 1$. Let $\beta = q_1$ then $w(\beta) = 1$. Thus

$$\mathcal{D} = \{0, q_1 - x_1 + 1\}.$$

$\square$

Corollary 6.6. *When $n = 2$, $|\mathcal{D}| = 3$ if and only if $x_2 = 2$.*

We have given the size and shape of the sets $\mathcal{D}$ and $\mathcal{E}$ for the $n = 2$ case. We now investigate these sets when $n = 3$.

6.5 The $n = 3$ case

Corollary 6.7. *For $n = 3$, we have six main cases to consider.*

Case 1: For $x_1 \neq 0$, $x_2 \neq 0$, $x_3 \neq 0$:

$$|\mathcal{D}| = \begin{cases} x_2 + 1 & \text{for } x_3 \leq \frac{1}{2}q_3 \\ x_2 + 2 & \text{otherwise;} \end{cases}$$

$$|\mathcal{E}| = q_2 + 4.$$

Case 2: For $x_1 = x_2 = 0$, $0 \leq x_3 \leq q_3 - 1$:

$$|\mathcal{D}| = \begin{cases} 1 & \text{for } x_3 \leq \frac{1}{2}q_3 \\ 2 & \text{otherwise;} \end{cases}$$

$$|\mathcal{E}| = q_2 + 3.$$

Case 3: For $x_1 = x_3 = 0$, $0 \leq x_2 \leq q_2$:

$$|\mathcal{D}| = x_2 + 1 \qquad |\mathcal{E}| = q_2 + 2.$$

Case 4: For $x_1 = 0$, $x_2 \neq 0$, $x_3 \neq 0$:

$$|\mathcal{D}| = \begin{cases} x_2 + 1 & \text{for } x_3 \leq \frac{1}{2}q_3 \\ x_2 + 2 & \text{otherwise;} \end{cases}$$

$$|\mathcal{E}| = q_2 + 3.$$

Case 5: For $x_2 = 0$, $x_1 \neq 0$, $0 \leq x_3 \leq q_3 - 1$:

$$|\mathcal{D}| = \begin{cases} q_2 + 1 & \text{for } x_3 < \frac{1}{2}q_3 \\ q_2 + 2 & \text{otherwise;} \end{cases}$$

$$|\mathcal{E}| = \begin{cases} 2q_2 + 2 & \text{if } x_3 = \frac{q_3 - 1}{2} \\ 2q_2 + 3 & \text{otherwise.} \end{cases}$$

Case 6: For $x_3 = 0$, $x_1 \neq 0$, $x_2 \neq 0$:

$$|\mathcal{D}| = x_2 + 1 \qquad |\mathcal{E}| = q_2 + 3.$$

Remark 6.8. *Note that in all but one case (i.e. when $x_2 = 0$, $x_1 \neq 0$) that $|D|$ is dependent on x_2. This may be surprising as the $|D|$ in Theorem 3 of [dST07] depends only on q_i, for even i. However, we note that in [dST07], they are concerned with the ring of integers - i.e. when $h = 0$, or in our co-ordinate language when $(x_1, \ldots, x_n) = (1, 0, \ldots, 0)$ - so we would have $x_2 = 0$ in this case. It is plausible, then, that $|D|$ is, in general, dependent not on the q_i but on the x_i.*

Proof. Case 1. If $x_1x_2x_3 \neq 0$, Propositions 5.12 and 5.13 give

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1q_2 + 1, p - \min(x_3, q_3 - x_3) \cdot s_2, p - \min(x_1, q_1 - x_1)\}$$

and

$$\mathcal{D} = \begin{cases} \{0, q_1 - x_1, 2q_1 - x_1, \ldots, x_2q_1 - x_1\} & \text{for } x_3 \leq \frac{1}{2}q_3 \\ \{0, q_1 - x_1, 2q_1 - x_1, \ldots, x_2q_1 - x_1, & \\ \qquad p - x_1 + q_1x_2 - (q_1q_2 + 1)x_3\} & \text{otherwise.} \end{cases}$$

Case 2. Let $x_1 = x_2 = 0$ and $0 \leq x_3 < q_3$. Proposition 5.13 shows us if $x_3 \leq \frac{1}{2}q_3$ then $\mathcal{D} = \{0\}$, but $\mathcal{D} = \{0, p - x_3 \cdot s_2\}$ otherwise. Proposition 5.12 gives us $\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1q_2 + 1, p - \min(q_3 - x_3, x_3) \cdot s_2\}$.

Case 3. Let $x_1 = x_3 = 0$, $0 \leq x_2 \leq q_2$. Then, by Propositions 5.12 and 5.13, we have

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1q_2 + 1\},$$

and

$$\mathcal{D} = \{0, q_1, 2q_1, \ldots, x_2 q_1\}.$$

Case 4. Let $x_1 = 0$, $x_2 \neq 0$, $x_3 \neq 0$. Then Proposition 5.13 gives us: $\mathcal{D} = \{0, q_1, 2q_1, \ldots, x_2 q_1\}$ when $x_3 \leq \frac{1}{2} q_3$ and $\mathcal{D} = \{0, q_1, 2q_1, \ldots, x_2 q_1, p + q_1 x_2 - x_3 \cdot s_2\}$ otherwise. Proposition 5.12 yields

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1 q_2 + 1, p - \min(x_3, q_3 - x_3) \cdot s_2)\}.$$

Case 5. Let $x_2 = 0$, $x_1 \neq 0$, and $0 \leq x_3 < q_3$. This case requires a little more care. If $x_3 = q_3 - 1$ then

$$\begin{aligned} d_3 &= *^{q_1+1-x_1} S_1^{q_2} S_2^{x_3} *^{x_1} \\ w_3 &= *^{q_1+1-x_1} S_1^{q_2} S_2^{x_3} *^{x_1}. \end{aligned}$$

Otherwise:

$$\begin{aligned} d_3 &= *^{q_1+1-x_1} S_1^{q_2-1} S_2^{q_3-2-x_3} L_2 S_2^{x_3} *^{x_1} \\ w_3 &= S_2^{\max(q_3-x_3-2, x_3)} L_2 S_2^{\min(q_3-x_3-2, x_3)} S_2 S_1^{q_2-1} *^{\max(q_1-x_1+1, x_1)} *^{\min(q_1-x_1+1, x_1)}. \end{aligned}$$

We claim:

$$\mathcal{D} = \begin{cases} \{0, q_1 - x_1 + 1, 2q_1 - x_1 + 1, \ldots, q_2 q_1 - x_1 + 1\} & \text{for } x_3 < \frac{1}{2} q_3 \\ \{0, q_1 - x_1 + 1, 2q_1 - x_1 + 1, \ldots, q_2 q_1 - x_1 + 1, & \\ \quad p - x_3(q_1 q_2 + 1) - x_1\} & \text{otherwise.} \end{cases}$$

By a simple extension of Proposition 5.13, we have $\{0, q_1 - x_1 + 1, 2q_1 - x_1 + 1, \ldots, q_2 q_1 - x_1 + 1\} \in \mathcal{D}$ whether $x_3 < \frac{1}{2} q_3$, or otherwise. When $x_3 < \frac{1}{2} q_3$, the string d_3 from the beginning of $S_2^{q_3 - x_3 - 2}$ onwards is an initial segment of w_3, so there can be no other elements in $\mathcal{D}$. Thus $\{0, q_1 - x_1 + 1, 2q_1 - x_1 + 1, \ldots, q_2 q_1 - x_1 + 1\} = \mathcal{D}$ in this case.

If $x_3 \geq \frac{1}{2} q_3$ then, by 5.13, we also get $p - x_3 s_2 - x_1 \in \mathcal{D}$.

Now consider the sets $\mathcal{E}$. When $x_3 \neq \frac{q_3 - 1}{2}$, we claim:

$$\begin{aligned} \mathcal{E} = \{&0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_2 q_1 + 1, p - \min(x_3 + 1, q_3 - x_3) \cdot s_2, \\ &p - 1 - (q_2 - 1) q_1, p - 1 - (q_2 - 2) q_1, \ldots, p - 1 - q_1, p - \min(q_1 - x_1 + 1, x_1)\}. \end{aligned}$$

By Proposition 5.12, we have $\{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1q_2 + 1, p - \min(x_3, q_3 - x_3) \cdot s_2\} \in \mathcal{E}$. Let α be the first element of $S_2^{\min(q_3 - x_3 - 2, x_3)}$. Then the string from α to the start of $S_1^{q_2-1}$ is an initial segment of w_3. However, the first element of the second S_1 would then line up with the last element of an L_1 (either from another S_2 or the L_2 block). This shifts the rest of the string out of line, thus $\{p - 1 - (q_2 - 1)q_1, p - 1 - (q_2 - 2)q_1, \ldots, p - 1 - q_1, p - \min(q_1 - x_1 + 1, x_1)\} \in \mathcal{E}$. As there are no other candidates, we have the required result.

When $x_3 = \frac{q_3-1}{2}$ we have:

$$\begin{aligned} d_3 &= *^{q_1+1-x_1} S_1^{q_2-1} S_2^{\frac{q_3-3}{2}} L_2 S_2^{\frac{q_3-1}{2}} *^{x_1} \\ w_3 &= S_2^{\frac{q_3-3}{2}} L_2 S_2^{\frac{q_3-1}{2}} S_1^{q_2-1} *^{\max(q_1+1-x_1, x_1)} *^{\min(q_1+1-x_1, x_1)} \end{aligned}$$

and we claim:

$$\begin{aligned} \mathcal{E} = \{&0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_2q_1 + 1, p - \frac{q_3 + 1}{2} \cdot s_2, \\ &p - 1 - (q_2 - 2)q_1, p - 1 - (q_2 - 3)q_1, \ldots, p - 1 - q_1, p - \min(q_1 - x_1 + 1, x_1)\}. \end{aligned}$$

Again, by Proposition 5.12, we have $\{0, 1, q_1+1, 2q_1+1, \ldots, q_1q_2+1, p-\frac{q_3+1}{2}\cdot s_2\} \in \mathcal{E}$. For the other elements, we use the same argument as above but since the number of S_2 blocks on the right side of the L_2 are greater than the number on the left, we have one extra S_1 element being an initial segment of w_3. This means we don't have the first element of either the first nor second S_1 blocks in $\mathcal{E}$, thus: $\{p - 1 - (q_2 - 1)q_1, p - 1 - (q_2 - 2)q_1, \ldots, p - 1 - q_1, p - \min(q_1 - x_1 + 1, x_1)\} \in \mathcal{E}$, as required.

Case 6. Let $x_3 = 0$, $x_1x_2 \neq 0$. Propositions 5.12 and 5.13 yield:

$$\mathcal{E} = \{0, 1, q_1 + 1, 2q_1 + 1, \ldots, q_1q_2 + 1, p - \min(x_1, q_1 - x_1)\},$$

and

$$\mathcal{D} = \{0, q_1 - x_1, 2q_1 - x_1, \ldots, x_2q_1 - x_1\}.$$

□

Corollary 6.9. *For $n = 3$, $|D| = 3$ if and only if*

$$\begin{cases} x_2 = 2 \text{ and } x_3 \leq \frac{1}{2}q_3; \text{ or} \\ x_2 = 1 \text{ and } x_3 > \frac{1}{2}q_3; \text{ or} \\ x_2 = 0, x_1 \neq 0 \text{ and } q_2 = 2 \text{ when } x_3 < \frac{1}{2}q_3, \text{ or } q_2 = 1 \text{ when } x_3 > \frac{1}{2}q_3. \end{cases}$$

Remark 6.10. *Recall for $\mathfrak{O}_L$, $|\mathcal{D}| = 1$ if and only if $|\mathcal{E}| \leq 3$ [dST07]. Clearly this is not the case for $\mathfrak{P}_L^h$ in general - in particular, the cases where $|\mathcal{E}|$ depends on q_i, for i even. For instance, when $n = 2$ we have the exceptional cases $x_2 = 0$ ($|\mathcal{E}| = q_2 + 1$) and $x_1 x_2 \neq 0$ ($|\mathcal{E}| = q_2 + 2$). Similarly, when $n = 3$, the exceptional cases are $x_1 = x_2 = 0$, $x_3 \leq \frac{1}{2}q_3$ ($|\mathcal{E}| = q_2 + 3$) and $x_1 = x_2 = x_3 = 0$ ($|\mathcal{E}| = q_2 + 2$).*

In this chapter we explored, case by case, the size and shape of $\mathcal{E}$ and $\mathcal{D}$ for $n = 1, 2$ and 3. We also conjectured further statements regarding the size and shape of $\mathcal{D}$ and $\mathcal{E}$ for all values of h, for general n. These can easily be seen to agree with the cases $n = 1, 2, 3$, but they remain conjectural for general n. In the concluding chapter we look at some consequences of Chapter 5.

Chapter 7

Consequences

This chapter aims to give some important consequences of the results from the previous chapters.

7.1 Ferton's Theorem in Characteristic p

Firstly, as we have the pattern of d_n and w_n in general, we can easily consider the conditions for which $d_n = w_n$, i.e., we can determine when $\mathfrak{P}^h$ is free over $\mathfrak{A}_{L/K}(\mathfrak{P}^h)$. Recall the Theorem from [Fer73], for $\mathrm{char}(K) = 0$:

Theorem 7.1. *Let K be a finite extension of $\mathbb{Q}_p$. Let L/K be a totally ramified, cyclic extension of degree p, with ramification number $t = q_0p + s$, and let $0 \leq h \leq p-1$.*

1. *If $t \equiv 0 \pmod{p}$, then $\mathfrak{P}^h$ is free over $\mathfrak{A}_{L/K}$ for all h.*
2. *If $t \equiv 1 \pmod{p}$ and if $1 \leq t < \frac{pe}{p-1} - 2$, then $\mathfrak{P}^h$ is free over $\mathfrak{A}_{L/K}$ if and only if $h = 0$, $h = 1$ or $h > \frac{p+1}{2}$.*
3. *If $t \not\equiv 0$, $t \not\equiv 1 \pmod{p}$, and:*
   (a) *If $1 \leq t < \frac{pe}{p-1} - 2$ and h satisfies $s < h \leq p-1$, then $\mathfrak{P}^h$ is not free over $\mathfrak{A}_{L/K}$.*

(b) *Let* $\frac{s}{p} = [q_0, q_1, \ldots, q_n]$, $q_n > 1$ *be shorthand for the continued fraction expansion, i.e.,*

$$\frac{s}{p} = q_0 + \frac{1}{q_1 + \ldots \frac{1}{\ldots + \frac{1}{q_n}}}.$$

If $1 \leq t < \frac{pe}{p-1} - 1$ *and* h *satisfies* $0 \leq h \leq s$, *then for* $s \neq 0$, $s \neq 1$, $\mathfrak{P}^h$ *is free over* $\mathfrak{A}_{L/K}$ *if and only if:*

- *for* n *even:* $h = s$ *or* $h = s - q_n$*;*
- *for* n *odd:* $s - \frac{1}{2}q_n \leq h \leq s$.

Note that Case 1 of Theorem 7.1 does not occur in characteristic p, since the residue field is perfect and we are assuming L/K is totally ramified. With this in mind, the results from this thesis indicate the analogous result of [Fer73] holds in characteristic p.

Corollary 7.2. *(Ferton's Theorem in char*$(K) = p$*) Let* $s - p + 1 \leq h \leq s$.

1. *If* $t \equiv 1 \pmod{p}$*, i.e.,* $s = 1$*, then* $\mathfrak{P}_L^h$ *is free over* $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ *if and only if* $\frac{1-p}{2} \leq h \leq 0$. *Taking* $p > 2$*, this inequality becomes* $\frac{3-p}{2} \leq h \leq 1$.

2. *If* $t \not\equiv 1 \pmod{p}$ *then:*

   (a) $\mathfrak{P}_L^h$ *is not free over* $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ *for all* $h < 0$*;*

   (b) *let* $\frac{s}{p} = [0; q_1, \ldots, q_n]$*, with* $q_n > 1$. *For* $h \geq 0$*, i.e.,* $0 \leq h \leq s$*,* $\mathfrak{P}_L^h$ *is free over* $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ *if and only if*

   - *for* n *even,* $h = s$ *or* $h = s - q_n$*;*
   - *for* n *odd,* $s - \frac{1}{2}q_n \leq h \leq s$.

Proof. Case 1. The condition $s = 1$ means $n = 1$ and $q_1 = p$. In this case we have $D = *^{q_1 - x_1} *^{x_1}$ and $W = *^{\max(q_1 - x_1, x_1)} *^{\min(q_1 - x_1 . x_1)}$. So $D = W$ if and only if $x_1 \leq q_1 - x_1$, i.e., if and only if $0 \leq x_1 \leq \frac{1}{2}p$. This corresponds to the values $h = 1, 0, \ldots, \frac{1-p}{2}$, as required.

Case 2. For a given continued fraction expansion $[q_0; q_1, \ldots, q_n]$, $\mathfrak{P}_L^h$ is free over $\mathcal{A}_{L/K}(\mathfrak{P}_L^h)$ if and only if $D = W$, for co-ordinates $(x_1, \ldots, x_n)$ corresponding to the value of $s - h$.

First let n be even and $h = s$. This means our co-ordinates will be $(x_1, \ldots, x_n) = (0, \ldots, 0)$. Clearly

$$D = L_{n-1} S_{n-1}^{q_n - 1},$$

and, by §5.3.2.1, we see that

$$W = \widehat{w}_n = L_{n-1} S_{n-1}^{q_n - 1}.$$

Thus $W = D$ in this case and therefore we have freeness when n is even and $h = s$.

Now let $h = s - q_n$ and let n remain even. The co-ordinate corresponding to $h = s - q_n$ is $(x_1, \ldots, x_n) = (0, \ldots, 0, 1, 0)$.

To obtain D, we move $x_{n-1} = 1$ S_{n-2} block from the left to the right of $L_{n-1} S_{n-1}^{q_n - 1}$. Since $L_{n-1} = S_{n-2}^{q_{n-1}} L_{n-2}$, we get:

$$\begin{aligned} D &= S_{n-2}^{q_{n-1} - 1} L_{n-2} S_{n-1}^{q_n - 1} S_{n-2} \\ &= S_{n-1} S_{n-1}^{q_n - 1} S_{n-2} \\ &= S_{n-1}^{q_n} S_{n-2}. \end{aligned}$$

Since the L_{n-1} block is broken, we use §5.3.2.2, with $t = 0$ and $x_n = 0$, to get - for $q_n \neq 1$ -

$$\widehat{w}_n = S_{n-1}^{q_n - 1} W_{n-1}.$$

Since no other blocks are broken or moved, in order to maximise W, we must have:

$$W = S_{n-1}^{q_n - 1} S_{n-1} S_{n-2} = S_{n-1}^{q_n} S_{n-2}.$$

If, however, $q_{n-1} = 1$,then $\widehat{w}_n = \emptyset$ and so $D \neq W$.

Thus $D = W$ when $h = s - q_n$, for $q_n > 2$. We therefore have freeness in the even case when $h = s$ or $h = s - q_n$, as long as $q_n > 1$.

Now let $s - q_n < h < s$. This corresponds to co-ordinates $(0, \ldots, 0, x_n)$, where $x_n \neq 0$. Then $D = S_{n-1}^{x_n} L_{n-1} S_{n-1}^{q_n - x_n - 1}$ and, since no level $n - 1$ block is broken, we use §5.3.2.1 to give:

$$W = \widehat{w}_n = L_{n-1} S_{n-1}^{q_n - 1}.$$

Since we require $x_n \neq 0$, $D \neq W$ and therefore we do not have freeness for n even, $s - q_n < h < s$.

Let us now consider the other cases. If n is even then $S_n = L_{n-1}S_{n-1}^{q_n-1}$ and we move x_n blocks of S_{n-1} from right to left, alternating until we move x_0 blocks of $*$ left to right (as in Algorithm 4.10). In all cases, w_n starts with L_{n-1} if possible, otherwise it will start with S_{n-1}. So then $w_n = d_n$ can only occur if

1. $x_1 = \ldots = x_n = 0$ (which we have already covered); or
2. the L_{n-1} block gets broken in D, so both d_n and w_n start with S_{n-1} (which can only happen when $x_n = 0$, $x_{n-1} = 1$ and $x_j = 0$, for $j < n-1$ and which, again, we have just covered); or
3. no complete L_{n-1} or S_{n-1} occurs in D. This last case can never happen since once we break either the L_{n-1} or an S_{n-1}, the blocks that become subsequently broken are just smaller blocks of that initial block we broke. So the L_{n-1} and a further $S_{n-1}^{q_n-2}$ blocks will remain intact - that is, $S_{n-1}^{q_n-1}$ blocks will remain intact.

This means when n is even we have freeness if and only if $h = s$ or $h = s - q_n$.

Now let $n \geq 3$ be odd. The co-ordinates corresponding to the range $s - \frac{1}{2}q_n \leq h \leq s$ are the consecutive $(0,\ldots,0)$, $(0,\ldots,0,1)$, $\ldots$, $(0,\ldots,0,\left\lfloor \frac{q_n}{2} \right\rfloor)$. When n is odd, we have $S_n = S_{n-1}^{q_n-1}L_{n-1}$, and in this case we have to move x_n lots of S_{n-1} from left to right, giving us:

$$D = S_{n-1}^{q_n-x_n-1}L_{n-1}S_{n-1}^{x_n}.$$

Since no level $n-1$ block is broken, we use §5.3.3.1 to see that, for $x_n < \frac{1}{2}q_n$:

$$W = \widehat{w}_n = S_{n-1}^{q_n-x_n-1}L_{n-1}S_{n-1}^{x_n}.$$

Thus $W = D$, and hence we have freeness, when n is odd and $s - \frac{1}{2}q_n \leq h \leq s$. If $s - q_n < h < s - \frac{1}{2}q_n$, we have instead:

$$W = S_{n-1}^{x_n-1}L_{n-1}S_{n-1}^{q_n-x_n}.$$

Thus, we do not have freeness for n odd and $s - q_n < h < s - \frac{1}{2}q_n$.

For the other cases, by §5.3.3, we have $\widehat{w}_n = S_{n-1}^M \ldots$, for some M. We know D has this form only if $x_n = 0, \ldots, q_n - 1$, and we have already shown $D = W$ only if $x_n \leq \frac{1}{2} q_n$.

Therefore, if n is odd, we have freeness if and only if $s - \frac{1}{2} q_n \leq h \leq s$.

□

Remark 7.3. *There are, of course, other ways to prove Ferton's Theorem in characteristic p, for example see the recent work of [Huy14].*

Remark 7.4. *It is interesting that, for degree p extensions, we always have freeness in the case $h = s$. To see what this corresponds to let $\mathfrak{D}^{-1}$ be the inverse different, then*

$$\mathfrak{P}^{-1}\mathfrak{D}^{-1} = \mathfrak{P}^{v},$$

where

$$\begin{aligned} v &= -1 - (p-1)(s-1) \\ &\equiv -1 + (s+1) \\ &\equiv s. \end{aligned}$$

Taking the dual over the trace we have:

$$\mathfrak{P}^{-1}\mathfrak{D}^{-1} \leftrightarrow \mathfrak{P}.$$

The second consequence we can obtain is Theorem 3 of [dST07]. As was shown in Remark 2.9, if $\frac{s}{p} = [0; q_1, \ldots, q_n]$ then $\frac{-s}{p} = [-1; 1, q_1 - 1, q_2, \ldots, q_n]$. Knowing this, Theorem 3 of [dST07] can be rewritten as:

Theorem 7.5. *Let $h = 0$. If $s = 0$ or $s = p - 1$ then $|D| = 1$. Otherwise*

$$|D| = 1 + \sum_{\substack{i \leq n \\ i \text{ even}}} q_i.$$

In our co-ordinate system we note that the case when $h = 0$ corresponds to $(1, 0, \ldots, 0)$. In fact, we can generalise this theorem further and say the following:

Theorem 7.6. *Let our co-ordinates be of the form $(x_1, 0, \ldots, 0)$, i.e., let h be any of $h = 0, -s, -2s, \ldots, -q_1 s$. If $s = 0$ or $s = p - 1$ then $|D| = 1$. Otherwise*

$$|D| = 1 + \sum_{\substack{i \leq n \\ i \text{ even}}} q_i.$$

Proof. This set of co-ordinates indicates we need to move x_1 lots of $*$ from left to right in the word $S_n = L_{n-1}S_{n-1}^{q_n-1}$ for the even n case, and in the word $S_n = S_{n-1}^{q_n-1}L_{n-1}$ in the odd n case. In both cases S_n begins with an L_1 block. Since $x_1 \leq q_1$, it will always be the first L_1 that is split. From the construction of our recursive relation of words, (4.1), (4.2) and (4.3), S_n will always begin with

$$(L_1 S_1^{q_2-1})^{q_3} \ldots = S_2^{q_3} \ldots$$

This means, after we have shifted x_1 lots of $*$ from left to right, our new word will be of the form

$$*^{q_1+1-x_1} S_1^{q_2-1} S_2^{q_3-1} L_2 S_3^{q_4-1} \ldots *^{x_1} .$$

This is essentially (4.18) but with x_i replaced by q_i, for even i. Our statement then follows from direct substitution into (5.11) and (5.12), since $x_n = 0 < \frac{1}{2}q_n$ in this case.

□

Bibliography

[Aib03] Akira Aiba. Artin-Schreier extensions and Galois module Structure. *J. Number Theory*, 102:118–124, 2003.

[BBF72] F. Bertrandias, J-P. Bertrandias, and M. J. Ferton. Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. *C.R. Acad. Sc. Paris*, 274:1388–1391, 1972.

[BE13a] Nigel Byott and G. Griffith Elder. Scaffolds and Generalized Integral Galois Module Structure. *arXiv:1308.2088[math.NT]*, 2013.

[BE13b] Nigel Byott and G. Griffith Elder. Sufficient Conditions for Large Galois Scaffolds. *arXiv:1308.2092 [math.NT]*, 2013.

[Ber73] A.M Bergé. Quelques résultats relatifs à l'ordre associé à une extension. *Publ. Math. Bordeaux*, 5:9–24, 1972-1973.

[BF72] F. Bertrandias and M. J. Ferton. Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local. *C.R. Acad. Sc. Paris*, 274:1330–1333, 1972.

[Byo99] Nigel Byott. Integral Galois module structure of some Lubin-Tate extensions. *Journal of Number Theory*, 77:252–273, 1999.

[Byo08] Nigel Byott. On the Integral Galois Module Structure of Cyclic Extensions of p-adic Fields. *Quart. J. Math.*, 59:149–162, 2008.

[CF67] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory.* Academic Press, 1967.

[Cha94] Robin Chapman. A Simple Proof of Noether's Theorem. *Glasgow Math. J.*, 38:49–51, 1994.

[dST07] Bart de Smit and Lara Thomas. Local Galois Module Structure in Positive Characteristic and Continued Fractions. *Arch. Math*, 88:207–219, 2007.

[Eld09] G. Griffith Elder. Galois Scaffolding In One-Dimensional Elementary Abelian Extensions. *American Mathematical Society*, 137(4):1193–1203, 2009.

[Fer73] M. J Ferton. Sur les idéaux d'une extension cyclique de degré premier d'un corps local. *C.R. Acad. Sc. Paris*, 276:Serie A –1483, 1973.

[FT91] A. Fröhlich and M.J. Taylor. *Algebraic Number Theory.* Cambridge University Press, 1991.

[Huy14] Duc Van Huynh. Artin-Schreier Extensions and Generalized Associated Orders. *Journal of Number Theory*, 136:28–45, 2014.

[Leo59] H. W. Leopoldt. Uber die Hauptordnung der ganzen Elementen eines abelschen Zahlkorpers. *J. Reine Angew. Math.*, 201:119–149, 1959.

[Let05] G. Lettl. Note on a Theorem of A. Aiba. *J. Number Theory*, 115:87–88, 2005.

[Miy98] Y. Miyata. On the Module Structure of Rings of Ideals in p-adic Number Fields Over Associated Orders. *Math. Proc. Camb. Phil. Soc.*, 123:199, 1998.

[Noe32] Emmy Noether. Normalbasis bei Körpern ohne höhere Verzweigung. *Crelle*, 167:147–152, 1932.

[Ser68] J-P. Serre. *Local Fields.* Springer-Verlag, 1968.

[Tho10] Lara Thomas. On the Galois Module Structure of Extensions of Local Fields. *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 157–194, 2010.