Continued fractions of Laurent series with partial quotients from a given set

by

ALAN G.B. LAUDER*(London)

March 11, 1999

*The author is an EPSRC CASE student sponsored by the Vodafone Group. He also gratefully acknowledges the support of the US-UK Fulbright Commission, and thanks the anonymous referee for several helpful comments.

Running title. Continued Fractions, Laurent Series.
1991 Mathematics Subject Classification. Primary 11J61, 11J70; Secondary 11T55, 11T71.
Key words and phrases. Continued fractions, Finite fields, Laurent series, Linear complexity profiles, Sequences.

1 Introduction

Van der Poorten and Shallit's paper [10] begins "it is notorious that it is damnably difficult to explicitly compute the continued fraction of a quantity presented in some other form". The quantity is usually presented either as a power series or as the root of a specific equation. There has been some success in the former case for continued fractions of real numbers, such as Euler's famous continued fraction for e [11] and more recent work [10] on "folded" continued fractions; however, other than the well-known results for quadratic real numbers, the only success with the latter has been for continued fractions of Laurent series rather than real numbers. In this paper we continue this line of investigation. We consider families of continued fractions of Laurent series whose partial quotients all lie in a given set. Following ideas of Baum and Sweet [2], we show that one may describe the zeros of certain collections of equations in terms of such families. The paragraphs that follow introduce the notation and definitions necessary to give a fuller description of our results.

Let $\mathbb{F}_q$ be the finite field with q elements and L_q denote the field of formal Laurent series in x^{-1} over $\mathbb{F}_q$ given by

$$L_q = \left\{ \sum_{i \geq n} \alpha_i x^{-i} \mid n \in \mathbb{Z}, \alpha_i \in \mathbb{F}_q \right\}.$$

We have the inclusions $\mathbb{F}_q[x] \subset \mathbb{F}_q(x) \subset L_q$. Elements in $\mathbb{F}_q(x)$ are called rational, and those which lie in L_q but not in $\mathbb{F}_q(x)$ are called irrational. We define a norm on L_q as follows: If $\alpha \in L_q$ is non-zero then we may write $\alpha = \sum_{i \geq n} \alpha_i x^{-i}$ where $\alpha_n \neq 0$. In this case we define $|\alpha| = q^{-n}$. If $\alpha = 0$ we define $|\alpha| = 0$. Observe that if $\alpha = s/t$ is a rational Laurent series with $s, t \in \mathbb{F}_q[x]$ then $|\alpha| = q^{\deg s - \deg t}$. We define P_q to be the ring of all $\alpha \in L_q$ with $|\alpha| < 1$, and we will frequently abbreviate L_q and P_q to L and P.

It is easy to verify that a continued fraction theory exists for the field L [1, 5]; in particular, any irrational Laurent series f in L has a unique infinite continued fraction expansion

$$f = a_0 + 1/(a_1 + 1/(a_2 + 1/(\ldots)))$$

where $a_j \in \mathbb{F}_q[x]$ with $\deg a_j \geq 1$ for $j \geq 1$. We write $f = [\,a_0; a_1, a_2, \ldots]$. We call the polynomials a_j $(j \geq 0)$ the *partial quotients* of f, and a_0 is also referred to as the *polynomial part* of f. Any irrational Laurent series in P will have a zero polynomial part. It is these elements of L with which we shall be primarily concerned. The significance of the continued fraction expansion of a Laurent series is that one may use it to define a sequence of rational functions which are "best approximations" to that Laurent series. Laurent series whose continued fractions have partial quotients of "small degree" are of particular interest as these may be thought of as being "difficult to approximate". Such Laurent series arise naturally in applications relating to the study of the linear complexity properties of sequences over finite fields [8], and pseudorandom number generation [7].

Let S be a finite subset of $\mathbb{F}_q[x]$, and $CF(S) \subseteq P$ be given by

$$CF(S) = \{[\,0; a_1, a_2, \ldots] \mid a_j \in S,\ \deg a_j \geq 1\}\,.$$

So $CF(S)$ is the set of all infinite continued fractions which have a zero polynomial part and whose remaining partial quotients lie in S. We begin with a result for arbitrary finite fields which describes the number of expressions $\alpha_1 x^{-1} + \ldots + \alpha_m x^{-m}$ which occur as the initial segment of a Laurent series in $CF(S)$ in terms of a generating function. This result, Proposition 5, is not only of some independent interest, but is a vital ingredient in the sections which follow. We now describe the main theorem. For a fixed $u \in \mathbb{F}_q[x]$ where $\operatorname{char} \mathbb{F}_q = 2$, let I_u denote the set of all $f \in P$ for which there exists $g \in L$ with

$$f^2 + uf + (1 + xg^2) = 0.$$

We first show, Lemma 7, that one may construct non-empty sets S so that $CF(S) \subseteq I_u$. Moreover, an application of Proposition 5 allows us to prove that for certain u there exists associated sets S such that $CF(S) = I_u$; more precisely, we prove

Theorem 1 *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $u \in \mathbb{F}_q[x]$. Then $I_u = CF(S)$ if and only if S is equivalent to a maximal solution group for u. That is to say, $\deg u \geq 1$ and S is a set of polynomials which satisfies the following criteria.*

1. *For each $v \in S$ of degree at least 1 there exists $w \in \mathbb{F}_q[x]$ with $v^2+uv = xw^2$.*

2. *The number s_m of polynomials of degree $m \geq 1$ in S is:*
   For $\deg u$ *even*
$$s_m = \begin{cases} (q-1)q^{(m-1)/2} & \textit{for } m \textit{ odd and less than } \deg u \\ 0 & \textit{for } m \textit{ even or } m \textit{ greater than } \deg u \\ q^{m/2} & \textit{for } m = \deg u \end{cases}$$
   For $\deg u$ *odd*
$$s_m = \begin{cases} (q-1)q^{m/2} & \textit{for } m \textit{ even and less than } \deg u \\ 0 & \textit{for } m \textit{ odd or } m \textit{ greater than } \deg u \\ q^{(m+1)/2} & \textit{for } m = \deg u \end{cases}$$

We determine all u which satisfy the conditions of Theorem 1 in Propositions 13, 14, 15 and Table 1. The case $u = x+1$ over $\mathbb{F}_2$ is a well-known result due to Baum and Sweet [2] which has an application in the study of binary sequences. Our new results have similar applications which we discuss in Section 5.2. We also show in Corollary 16 that for "many" values of d, there exist Laurent series in L_4 which are algebraic over $\mathbb{F}_4(x)$ of degree d, and which have partial quotients of bounded degree in their continued fraction expansion.

The remainder of the paper is organised in the following way. We gather some technical lemmas and a definition in Section 2. The first two lemmas will be used in Section 3 to determine the cardinality of sets of the form $CF(S)$ up to a given rational approximation. The final one is used in the proof of Theorem 1. Section 4 contains the proof of Theorem 1 as well as several related propositions. Finally, we present two different applications of Theorem 1 in Section 5.

2 Preliminaries

In this paper, we shall assume a familiarity with the basic notions from the theory of continued fractions of Laurent series. These can be gleaned from the detailed exposition of this theory given in [1, 5].

2.1 Lemmas

This section does not contain any essential definitions, and the reader may move directly onto Section 2.2 and refer back when required. We begin with a technical lemma which shall be used in the proof of the first part of Proposition 5.

Lemma 2 *Let* $f = [\,0; a_1, a_2, \ldots]$ *and* $f' = [\,0; a'_1, a'_2, \ldots]$ *where* $a_j, a'_j \in \mathbb{F}_q[x]\,(j \geq 1)$*. Suppose that* $a_j = a'_j$ *for* $1 \leq j \leq s-1$ *and* $a_s \neq a'_s$*. Let* $\sum_{1\leq j\leq s-1} \deg a_j = \sigma$*. Then*

$$|f - f'| = \frac{|a_s - a'_s|}{q^{2\sigma}|a_s||a'_s|}.$$

Proof: For $j \geq 1$, let m_j/n_j denote the j^{th} convergent to $[\,0; a_1, a_2, \ldots]$. So $m_j/n_j = [\,0; a_1, a_2, \ldots, a_j]$ with $\gcd(m_j, n_j) = 1$.
Let $\alpha = [\,a_s; a_{s+1}, a_{s+2}, \ldots]$ and $\alpha' = [\,a'_s; a'_{s+1}, a'_{s+2}, \ldots]$. Then [11, page 4]

$$f = \frac{\alpha m_{s-1} + m_{s-2}}{\alpha n_{s-1} + n_{s-2}},\ f' = \frac{\alpha' m_{s-1} + m_{s-2}}{\alpha' n_{s-1} + n_{s-2}}.$$

Hence

$$f - f' = \frac{(-1)^{s-2}(\alpha - \alpha')}{(\alpha n_{s-1} + n_{s-2})(\alpha' n_{s-1} + n_{s-2})},$$

where we use the well-known relation $m_{s-1}n_{s-2} - n_{s-1}m_{s-2} = (-1)^{s-2}$. The result now follows since $|\alpha| = |a_s|$, $|\alpha'| = |a'_s|$ and $|n_{s-1}| = q^{\sigma}$.

□

For any complex function $h(z)$ which is analytic in some region, let $[z^n]h(z)$ denote the coefficient of z^n in the power series expansion of $h(z)$. The next result is well-known and can be found in [9, Theorem 10.2]. It shall be useful in the proof of the second part of Proposition 5.

Lemma 3 *Let* $h(z)$ *be a complex function which is analytic in the disk* $\|z\| < R$*, where* $\|\ \|$ *denotes the complex modulus and* $R \in \mathbb{R}$*. Then for any* $r \in \mathbb{R}$ *with* $0 < r < R$ *and any* $n \in \mathbb{Z}$ *with* $n \geq 0$ *we have*

$$\|[z^n]h(z)\| \leq r^{-n} \max_{\|z\|=r} \|h(z)\|.$$

Proof: From the Cauchy integral formula we have that $[z^n]h(z) = \dfrac{1}{2\pi i}\displaystyle\int_\Gamma \frac{h(z)}{z^{n+1}}\,dz$ where Γ is any closed contour in the disk $\{z \in \mathbb{C} \mid \|z\| < R\}$ that contains the origin inside it and is positively orientated (traversed in a counter-clockwise direction). Taking Γ to be the circle centre the origin radius r gives us the result.

$\square$

We conclude with a result which we shall appeal to in the proof of Lemma 10. For a polynomial $f \in \mathbb{F}_q[x]$ the coefficient of x^n in f is denoted $[x^n]f$.

Lemma 4 *Let $W \subseteq \mathbb{F}_q[x]$ and let a be an odd positive integer and b an arbitrary integer with $b \geq a$. Denote by $n_b(W)$ the number of elements $c \in \mathbb{F}_q$ such that $c = [x^b]f$ for some $f \in W$. Suppose that*

1. *Each polynomial in W has degree not greater than b.*

2. *If $v, v' \in W$ then the degree of $v - v'$ is an odd number at least a.*

Then $\#(W) \leq n_b(W)q^{\lceil (b-a)/2 \rceil}$.

Proof: For each $c \in \mathbb{F}_q$, let $W(c)$ denote the set of all polynomials f in W with $[x^b]f = c$. If $W(c) \neq \emptyset$ then we may choose $f_c \in W(c)$. Let $V(c) = f_c - W(c)$. Then by property *2* of W, any two polynomials in $V(c)$ differ in some coefficient x^d where d is odd and $a \leq d$. Furthermore $d < b$ by property *1*. There are $\lceil (b-a)/2 \rceil$ such odd numbers d. So the cardinality of $V(c)$ is not greater than $q^{\lceil (b-a)/2 \rceil}$. Thus $\#(W(c)) = \#(V(c)) \leq q^{\lceil (b-a)/2 \rceil}$. Hence $\#(W) = \sum_c \#(W(c)) \leq n_b(W)q^{\lceil (b-a)/2 \rceil}$ as required

$\square$

2.2 An equivalence relation on sets of polynomials

We define the following equivalence relation on finite subsets of $\mathbb{F}_q[x]$: We say that S and T are *equivalent* if $\{a \in S \mid \deg a \geq 1\} = \{a \in T \mid \deg a \geq 1\}$. So if S and T are equivalent, then $CF(S) = CF(T)$ (the converse is also true). It will be convenient for us to consider sets $CF(S)$ where S contains polynomials of degree zero and zero itself. Any set T which is equivalent to such a set S will give us the same collection of continued fractions $CF(T)$ ($= CF(S)$), and we will make frequent use of this simple equivalence relation in the statements of the results which follow.

3 The cardinality of $CF(S)$ up to a given rational approximation

Let S be a finite set of polynomials in $\mathbb{F}_q[x]$. We wish to count the number of elements in $CF(S)$ up to a given rational approximation. To be more precise, for each $m \in \mathbb{N}$ we define an equivalence relation $\sim_m$ on L by

$$f \sim_m f' \Leftrightarrow |f - f'| < q^{-m}.$$

We consider the equivalence relation $\sim_m$ restricted to $CF(S)$ and denote the set of equivalence classes by $CF(S)/\sim_m$. So if $f,\ f' \in CF(S)$ then $f \sim_m f'$ if and only if the first m coefficients in the Laurent series expansions of f and f' agree. Proposition 5 describes the number of equivalence classes mod$\sim_m$ ($m \geq 1$) in $CF(S)$ in terms of a generating function which we construct in the paragraphs which follow. This result is not only of some interest in its own right, but is also a crucial ingredient in the proof of Theorem 1.

We make the following definitions: for $i \geq 1$ let v_i denote the number of polynomials in S of degree i and let the *degree enumerator* $f_S(z)$ of S be given by

$$f_S(z) = \sum_{i \geq 1} v_i z^i \in \mathbb{C}[z].$$

For $i \geq 1$, define the equivalence relation $\approx_i$ on S in the following way. Let $v, v' \in S$. Define $v \approx_i v'$ if

$$(1/v) \sim_{2i-1} (1/v').$$

Observe that polynomials of degree less than or equal to i lie in equivalence classes of size 1. We shall not be interested in those polynomials, but instead are concerned with polynomials of degree greater than i in S. We define w_i

to be the number of $\approx_i$-equivalence classes of polynomials of degree greater than i in S. Thus w_i is the cardinality of the largest subset of polynomials of degree greater than i in S which lie in distinct $\approx_i$-equivalence classes. Defining $w_0 = 1$ we let the *deficiency polynomial* $g_S(z)$ of S be given by

$$g_S(z) = \sum_{i \geq 0} w_i z^i \in \mathbb{C}[z].$$

Observe that if S and T are equivalent sets (according to Section 2.2) then $f_S(z) = f_T(z)$ and $g_S(z) = g_T(z)$. We write $f(z)$ and $g(z)$ for $f_S(z)$ and $g_S(z)$ when there is no risk of confusion.

Recall that the coefficient of z^n in $g(z)/(1-f(z))$ is denoted $[z^n]g(z)/(1-f(z))$. Also, let $\lceil m/2 \rceil$ denote the least integer which is not less than $m/2$; so $\lceil m/2 \rceil = (m+1)/2$ when m is odd, and $m/2$ when m is even. We may now state the main result of this section.

Proposition 5 *Let m be an odd positive integer. Then the cardinality of $CF(S)/\sim_m$ is $[z^{\lceil m/2 \rceil}]g(z)/(1-f(z))$. If the root [roots] of $1-f(z)$ with the smallest complex modulus has [have] modulus R, then for any $\varepsilon > 0$ there exists a constant $c \in \mathbb{R}$ such that the cardinality of $CF(S)/\sim_m$ is bounded above by $c(1/(R-\varepsilon))^{\lceil m/2 \rceil}$.*

Proof: We begin by proving the first statement of the proposition. Let m be an odd positive integer. For any $f = [\,0; a_1, a_2, \ldots]$ define the m^{th}*-deficiency* of f to be the unique integer k such that $\lceil m/2 \rceil - k = \sum_{1 \leq j \leq l} \deg a_j \leq \lceil m/2 \rceil < \sum_{1 \leq j \leq l+1} \deg a_j$. We first claim that any two elements f, f' in $CF(S)$ with m^{th}-deficiencies k and k' respectively, where $k \neq k'$, must lie in different equivalence classes mod $\sim_m$. For suppose $f = [\,0; a_1, a_2, \ldots]$ and $f' = [\,0; a'_1, a'_2, \ldots]$ lie in $CF(S)$, with $\sum_{1 \leq j \leq l} \deg a_j = \lceil m/2 \rceil - k$, $\sum_{1 \leq j \leq l'} \deg a'_j = \lceil m/2 \rceil - k'$ where $\deg a_{l+1} > k$, $\deg a'_{l'+1} > k'$ and $k \neq k'$. Let $j = s$ be the minimum integer for which $a_j \neq a'_j$. Then certainly $s \leq \min\{l, l'\} + 1$, and by Lemma 2 we have that $|f - f'| = \dfrac{|a_s - a'_s|}{q^{2\sigma}|a_s||a'_s|}$ where $\sigma = \sum_{1 \leq j \leq s-1} \deg a_j$. Since f and f' have different m^{th}-deficiencies, at least one of $\deg a_s$ and $\deg a'_s$ is strictly less than $\lceil m/2 \rceil - \sigma$. So suppose $\deg a_s \leq \deg a'_s$ with $\deg a_s < \lceil m/2 \rceil - \sigma$. If $\deg a_s = \deg a'_s$ then both are less than $\lceil m/2 \rceil - \sigma$ and so $|f - f'| > q^{-2\lceil m/2 \rceil} \geq q^{-m-1}$. Otherwise $\deg a_s < \deg a'_s$ and $|f - f'| = q^{-2\sigma - \deg a_s} > q^{-\sigma - \lceil m/2 \rceil}$. But certainly $\sigma < \lceil m/2 \rceil$ and so $|f - f'| > q^{-2\lceil m/2 \rceil} \geq q^{-m-1}$. This proves the claim.

Let $CF_k(S)\,(0 \leq k \leq \lceil m/2 \rceil)$ be the set of all elements in $CF(S)$ with m^{th}-deficiency k. We have shown that the number of equivalence classes of $CF(S)/\sim_m$ is equal to the summation over $k\,(0 \leq k \leq \lceil m/2 \rceil)$ of the number of equivalence classes of $CF_k(S)/\sim_m$.

Consider now the set of continued fractions $CF_k(S)$ for some $0 \leq k \leq \lceil m/2 \rceil$. Let $f,\, f' \in CF_k(S)$ with $f = [\,0; a_1, a_2, \ldots]$ and $f' = [\,0; a'_1, a'_2, \ldots]$ where $\sum_{1 \leq j \leq l} \deg a_j = \sum_{1 \leq j \leq l'} \deg a'_j = \lceil m/2 \rceil - k$ and $\deg a_{l+1}$, $\deg a'_{l'+1} > k$. If $a_j \neq a'_j$ for some $j\,(1 \leq j \leq \min\{l, l'\})$ then a similar argument to the one in the first paragraph of the proof shows that $f \not\sim_m f'$. Otherwise $l = l'$ and $a_j = a'_j\,(1 \leq j \leq l)$. In this case by Lemma 2, f and f' are in different $\sim_m$-classes if and only if $\dfrac{|a_{l+1} - a'_{l+1}|}{|a_{l+1}||a'_{l+1}|} \geq q^{-2k+1}$. But this latter condition is equivalent to $|(1/a_{l+1}) - (1/a'_{l+1})| \geq q^{-2k+1}$, that is to say, $a_{l+1} \not\approx_k a'_{l+1}$. (Here we need the fact that m is odd. We refer the reader to the paragraphs following this proof for a brief discussion of slight modification we need to make in the case m even.) So the cardinality of $CF_k(S)/\sim_m$ is the number of ways of selecting polynomials a_j in S of degree at least 1 whose degrees sum to $\lceil m/2 \rceil - k$, multiplied by the number of $\approx_k$-equivalence classes in S of polynomials of degree greater than k. (There are two exceptions to this: in the case $k = 0$ we actually "multiply" the number of ways of selecting non-constant polynomials in S whose degrees sum to $\lceil m/2 \rceil$ by 1; when $k = \lceil m/2 \rceil$ we take the number of ways of selecting no polynomials whose degrees sum to zero to be 1.) The latter is simply w_k, the coefficient of z^k in $g(z)$. The former is the coefficient of $z^{\lceil m/2 \rceil - k}$ in $\sum_{i \geq 0} f(z)^i = 1/(1 - f(z))$. Thus the cardinality of $CF(S)/\sim_m$ is the summation of this product over k, which is the coefficient of $z^{\lceil m/2 \rceil}$ in $g(z)/(1 - f(z))$. (See [13, page 36] for a description of the "arithmetic" of generating functions.) This proves the first part of the proposition.

To prove the second part, let $h(z) = g(z)/(1 - f(z))$. Then h is certainly analytic in the disk centre the origin of radius R, where R is the modulus of the "smallest" root [roots] of $1 - f(z)$. By Lemma 3, we have $\|[z^{\lceil m/2\rceil}](g(z)/(1-f(z)))\| = [z^{\lceil m/2\rceil}](g(z)/(1-f(z))) \leq c(1/(R-\varepsilon))^{\lceil m/2\rceil}$ where $\varepsilon > 0$ and $c = \max_{\|z\|=R-\varepsilon} h(z)$.

$\square$

To determine the cardinality of $CF(S)/\sim_m$ where m is even we must work with a slightly different generating function $\hat{g}(z)/(1-f(z))$. The polynomial $\hat{g}(z)(=\hat{g}_S(z)) = \sum_{i\geq 0} \hat{w}_i z^i$, which we call the *new deficiency polynomial*, is defined as follows. Let $\hat{w}_0 = 1$. For $i \geq 1$ and $v, v' \in S$ let $v \simeq_i v'$ if

$$(1/v) \sim_{2i} (1/v').$$

Let $\hat{w}_i$ denote the number of $\simeq_i$-equivalence classes of polynomials of degree greater than i in S. One may show that $\#(CF(S)/\sim_m)$ for m even is the coefficient of $z^{m/2}$ in $\hat{g}(z)/(1-f(z))$. Thus the statement of Proposition 5 remains true if we replace "m an odd positive integer" by "m an even positive integer". The proof in the even case is almost identical to that given for the odd case, except we must replace $g(z)$ by $\hat{g}(z)$ wherever it occurs, and make other appropriate minor changes. We shall only need the case m odd in the proof of the case of Theorem 1 which we explicitly give in Section 4.2, but in the outlined proof of the other case in Section 4.3 we use the new deficiency polynomial $\hat{g}(z)$.

4 Proof of Theorem 1 and related propositions

4.1 Preliminary results

Let $\operatorname{char} \mathbb{F}_q = 2$ and $u \in \mathbb{F}_q[x]$. Abbreviate L_q to L and P_q to P. We shall be concerned with the set of roots I_u which lie in P of equations of the form

$$X^2 + uX + (1 + xg^2)$$

where g is a suitably chosen element in L. Let $\deg u = t$. Suppose that for some g there exists $f \in P$ with $f^2 + uf + 1 = xg^2$. Then taking the norm of both sides we have $|g|^2 \leq q^{t-2}$. Conversely

Lemma 6 *For any $g \in L$ with $|g|^2 \leq q^{t-2}$ where $\deg u = t$ there exists a unique $f \in P$ with $f^2 + uf + (1 + xg^2) = 0$.*

Proof: Let $g \in L$ with $|g|^2 \leq q^{t-2}$. Let $u = \sum_{0 \leq j \leq t} u_j x^j$ and $xg^2 = \sum_{i \geq -(t-1)} h_i x^{-i}$. Observe that $h_i = 0$ for i even. We wish to show that there exists a unique $f = \sum_{i \geq 1} f_i x^{-i} \in P$ with $f^2 + uf + (1 + xg^2) = 0$. Consider the Laurent series $\sum_i f_i x^{-i}$ defined in the following way: Let $f_i = 0$ for $i \leq 0$ and determine f_i for $i \geq 1$ from the following recurrences (here $s \geq -(t-1)$).

$$\begin{cases} \sum_{0 \leq j \leq t} u_j f_{s+j} + f_{s/2}^2 = 0 & \text{for } s \text{ even, } s \neq 0 \\ \sum_{0 \leq j \leq t} u_j f_{s+j} + 1 = 0 & \text{for } s = 0 \\ \sum_{0 \leq j \leq t} u_i f_{s+j} + h_s = 0 & \text{for } s \text{ odd} \end{cases}$$

(The sequence f_i is consistently and uniquely defined because for each $s \geq -(t-1)$ the associated recurrence relation defines f_{s+t} uniquely in terms of the f_i with $i < s + t$.) The Laurent series $f = \sum_{i \geq 1} f_i x^{-i}$ then satisfies $f^2 + uf + (1 + xg^2) = 0$ by construction. This proves existence. Uniqueness follows from the observation that the sequence of coefficients of any $f \in P$ with $f^2 + uf + (1 + xg^2) = 0$ satisfies the above recurrences.

$\square$

Define $D_u = \{g \in L \mid |g|^2 \leq q^{t-2}\} = \{g \in L \mid |g| \leq q^{\lfloor t/2 \rfloor - 1}\}$. Let the map $\phi : D_u \to P$ be defined as follows: for $g \in D_u$ let $\phi : g \mapsto f$ where f is the unique Laurent series in P with $f^2 + uf + (1 + xg^2) = 0$. Denote the image of the map ϕ by I_u. Observe that the map ϕ is an injection since $\operatorname{char} \mathbb{F}_q = 2$ and so ϕ is a bijection from D_u to I_u. An equivalent description of I_u is the set of all $f \in P$ for which there exists $g \in L$ with $f^2 + uf + (1 + xg^2) = 0$.

The proof of the implication ($\Leftarrow$) in the following lemma, is based upon the proof of the first part of "Theorem 1" in Baum and Sweet [2].

Lemma 7 *Let $u \in \mathbb{F}_q[x]$ with $\operatorname{char} \mathbb{F}_q = 2$. Let S be a finite set of polynomials in $\mathbb{F}_q[x]$. Then $CF(S) \subseteq I_u$ if and only if for each polynomial $v \in S$ of degree at least 1 there exists $w \in \mathbb{F}_q[x]$ with $v^2 + uv = xw^2$.*

Proof: In this proof we use the equivalent description of I_u as the set of $f \in P$ for which there exists $g \in L$ such that $f^2 + uf + 1 = xg^2$.

($\Leftarrow$) Let $f = [\,0; a_1, a_2, \ldots]$ where $a_j \in S\,(j \geq 1)$ with $\deg a_j \geq 1$. For each $l \geq 0$ define $f_l = [\,0; a_1, a_2, \ldots, a_l, u, u, \ldots]$ where we use the obvious convention for $l = 0$. We prove by induction on l that there exists $g_l \in L$ with $f_l^2 + uf_l + 1 = xg_l^2$. If $l = 0$ then $f_0 = [\,0; u, u, \ldots]$ and so $(1/f_0) + u = f_0$ and $f_0^2 + uf_0 + 1 = 0$. We may therefore take $g_0 = 0$. Now suppose that $l = n > 0$. Then $(1/f_n) + a_1 = [\,0; a_2, \ldots, a_n, u, u, \ldots]$. So by induction, there exists g' such that

$$\{(1/f_n) + a_1\}^2 + u\{(1/f_n) + a_1\} + 1 = x(g')^2.$$

Hence

$$f_n^2 + uf_n + 1 = x\{f_n(g' + w)\}^2$$

where $a_1^2 + ua_1 = xw^2$.

Now $f = [\,0; a_1, a_2, \ldots]$. So $f = \lim_{l\to\infty} f_l$ where $f_l = [\,0; a_1, \ldots, a_l, u, u, \ldots]$. To each f_l there corresponds a unique g_l with $f_l^2 + uf_l + 1 = xg_l^2$. Taking limits we find that $f^2 + uf + 1 = xg^2$ where $g = \lim_{l\to\infty} g_l$. The field L is complete with respect to $|\,|$ and so $g \in L$ as required.

($\Rightarrow$) To prove the converse suppose that $f = [\,0; a_1, a_2, \ldots]$ where $a_j \in S\,(j \geq 1)$ with $\deg a_j \geq 1$, and $f^2 + uf + 1 = xg^2$ for some $g \in L$. Since $CF(S) \subseteq I_u$ there exists $g' \in L$ such that $f' = [\,0; a_2, a_3, \ldots]$ satisfies $(f')^2 + uf' + 1 = x(g')^2$. Now $f' = (1/f) + a_1$ and so $(a_1^2 + ua_1) = x(g'f + (g/f))^2$. The righthand side contains only odd powers of x and so there must exist $w \in \mathbb{F}_q[x]$ with $a_1^2 + ua_1 = xw^2$. Since a_1 was a arbitrary non-constant polynomial of S this completes the proof.

$\square$

(Observe that if $\deg u = 0$ or $u = 0$ then if $v^2 + uv$ contains no even powers of x we must have that $\deg v = 0$ or $v = 0$. But if S is a set which does not contain any polynomials of degree greater than zero then $CF(S) = \emptyset$. Thus the cases $\deg u = 0$ and $u = 0$ are of no interest and we assume for the remainder of the paper that $\deg u \geq 1$.)

Lemma 7 motivates Section 4.2 in which we study the pairs of polynomials v and w in $\mathbb{F}_q[x]$ which satisfy $v^2 + uv = xw^2$ for some fixed $u \in \mathbb{F}_q[x]$. We show that there is a bound on the number of pairs which can occur, and when and only when this bound is met we have that $CF(S) = I_u$ for some suitably chosen $S \subseteq \mathbb{F}_q[x]$. We prove this by considering the cardinality of the set of equivalence classes $CF(S)/\sim_m$ (where S is the appropriate set) and so must first determine the forms of $f_S(z)$ and $g_S(z)$ to make use of Proposition 5.

4.2 The case $\deg u$ even

It is easier to treat the cases $\deg u$ even and $\deg u$ odd separately, although the analysis in each case is essentially the same. In this section, we consider the former case, and briefly discuss the latter in the next section.

Let $\deg u = t$ be a positive even number. We are interested in determining the solutions in $\mathbb{F}_q[x] \times \mathbb{F}_q[x]$ of the equation $X^2 + uX + xY^2 = 0$ where $\operatorname{char} \mathbb{F}_q = 2$. Observe that if (v, w) is such a solution, then w is uniquely determined by v (since squaring is an automorphism in $\mathbb{F}_q$). We therefore define the set $G(u)$ to be the set of all $v \in \mathbb{F}_q[x]$ for which there exists $w \in \mathbb{F}_q[x]$ with $v^2 + uv = xw^2$. (It is convenient to include polynomials of degree 0 and 0 itself in $G(u)$, although these polynomials do not occur as partial quotients of continued fractions in $CF(G(u))$.) For the sake of notational simplicity, we occasionally abbreviate $G(u)$ to G. For $m \geq 0$, let G_m denote the set of all polynomials in G of degree less than or equal to m, and V_m the set of polynomials in G with degree exactly m. Define $G_{-1} = \{0\}$.

Lemma 8 *The set G is an elementary abelian 2-group under addition and the sets G_m are subgroups with $G = G_t$. Furthermore, $\#(G_m/G_{m-2}) \leq q$ for $1 \leq m \leq t-1$ and $\#(G_t/G_{t-1}) = 2$.*

Proof: It is easy to see that the set G is an elementary abelian 2-group with the sets G_m as subgroups. We claim that G does not contain any elements of even degree except those elements of degree t. For if v has even degree not equal to t then the leading term of v^2+uv has even degree, and so no polynomial w can exist with $v^2+uv = xw^2$. Thus $G_m = G_{m-1}$ for m even. Similarly G does not contain any polynomials of odd degree greater than t.

Thus $G = G_t$. To prove the remaining remarks, it suffices to consider the case m odd with m less than t. Suppose that $\#(G_m/G_{m-2}) > q$ where m is odd with $1 \leq m \leq t-1$. Then G_m/G_{m-2} must contain elements of the form $\gamma x^m + \gamma' x^{m-1} + G_{m-2}$ and $\gamma x^m + \gamma'' x^{m-1} + G_{m-2}$ where $\gamma, \gamma', \gamma'' \in \mathbb{F}_q$ with $\gamma' \neq \gamma''$. But then $(\gamma' - \gamma'')x^{m-1} + G_{m-2} \in G_m/G_{m-2}$ and so G_m contains a polynomial of even degree. This is a contradiction since $m \leq t-1$. To prove the final claim, we first observe that 0, $u \in G$ and so $\#(G_t/G_{t-1}) \geq 2$. Suppose that $\#(G_t/G_{t-1}) > 2$. Then G_t contains an element v whose leading coefficient $l(v)$ differs from the leading coefficient $l(u)$ of u. But since $v^2 + uv$ contains only odd powers of x, we have that $l(u)^2 + l(u)l(v) = 0$, which implies $l(u) = l(v)$. This contradiction establishes the final claim and completes the proof.

□

We call the set $G = G(u)$ the *full solution group* for u, and a subset of G a *solution set* for u. If G meets the bounds imposed by the above lemma then we say that G is a *maximal solution group*.

Lemma 9 *Let $u \in \mathbb{F}_q[x]$ have even degree $t \geq 2$ where $\operatorname{char} \mathbb{F}_q = 2$, and suppose that $G(u)$ is a maximal solution group for u. Then the degree enumerator $f(z)$ of $G(u)$ is given by*

$$f(z) \quad = \sum_{\substack{1 \leq i \leq t-1 \\ i \text{ odd}}} (q-1)q^{(i-1)/2} z^i + q^{t/2} z^t$$

and we have the factorisation

$$1 - f(z) \quad = \quad (1 - qz) \sum_{\substack{0 \leq i \leq t-2 \\ i \text{ even}}} q^{i/2}(z^i + z^{i+1}).$$

Proof: Recall that $V_m = \{v \in G \mid \deg v = m\}$. So the m^{th} coefficient $(m \geq 1)$ of $f(z)$ is $v_m = \#(V_m)$. As we observed in the proof of the preceding lemma, for m even and not equal to t, and for m odd and greater than t, we have $\#(V_m) = 0$. For m odd and less than t, $\#(V_m) = \#(G_m) - \#(G_{m-1}) = \#(G_m) - \#(G_{m-2})$ since $\#(G_{m-1}) = \#(G_{m-2})$. Now $\#(G_{-1}) = 1$ and since G meets the bounds imposed by the previous lemma we have that $\#(G_m/G_{m-2}) = q$ for m odd with $1 \leq m \leq t-1$. An easy induction argument establishes that $\#(G_m) = q^{(m+1)/2}$ and furthermore since $\#(G_t/G_{t-1}) = 2$ we have that $\#(G_t) = 2q^{t/2}$. So $\#(V_m) = (q-1)q^{(m-1)/2}$ for m odd and less than t. Similarly $\#(V_t) = \#(G_t) - \#(G_{t-1}) = 2q^{t/2} - q^{t/2} = q^{t/2}$. The factorisation is easy to verify.

$\square$

(We in fact have the fuller factorisation

$$1 - f(z) = (1-qz)(1+z) \prod_{1 \leq s \leq (t/2)-1} (qz^2 - \exp 2\pi i s/(t/2)).$$

It is somewhat curious that the roots of $1-f$ have complex modulus $1/q, 1/\sqrt{q}$ and 1, although this observation plays little part in what follows.)

Having determined the form of the degree enumerator polynomial $f(z)$ in the case that G is a maximal solution group, we now wish to find the form of the deficiency polynomial $g(z)$. We show in Lemma 10 that $g(z)$ is actually equal to the cofactor of $1-qz$ in the factorisation of $1-f(z)$, and so $g(z)/(1-f(z)) = (1-qz)^{-1}$. Using Proposition 5 we then see in Lemma 11 that the cardinality of $CF(G)/\sim_{2n-1}$ when G is a maximal solution group is q^n. This allows us to prove Lemma 12, which is the main result of Section 4.2.

Lemma 10 *Let $u \in \mathbb{F}_q[x]$ have positive even degree t where* $\operatorname{char} \mathbb{F}_q = 2$*, and suppose that $G(u)$ is maximal. Then the deficiency polynomial $g(z)$ of $G(u)$ is given by*

$$g(z) \quad = \sum_{\substack{0 \leq i \leq t-2 \\ i\, even}} q^{i/2}(z^i + z^{i+1})$$

Proof: Let $g(z)$ denote the deficiency polynomial of $G = G(u)$ and w_i $(i \geq 0)$ the coefficient of z^i in $g(z)$. Certainly $w_i = 0$ for $i \geq t$ and by definition $w_0 = 1$. For $1 \leq i \leq t-1$ we must establish that

$$w_i = \begin{cases} q^{i/2} & \text{when } i \text{ is even,} \\ q^{(i-1)/2} & \text{when } i \text{ is odd.} \end{cases}$$

We first show that $w_i \le q^{\lfloor i/2 \rfloor}$ $(1 \le i \le t-1)$ by considering the number of polynomials of each degree in a subset $W^{(i)} \subseteq G$ of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes. We then argue that this bound can be met by considering the structure of the maximal solution group G.

Suppose that $W^{(i)} \subseteq G$ is a set of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes. Let $W_s^{(i)}$ denote the subset of polynomials in $W^{(i)}$ which have degree s. Then $\#(W^{(i)}) = \sum_{s>i} \#(W_s^{(i)})$. Since $W^{(i)} \subseteq G$, $\#(W_s^{(i)}) = 0$ if $s > t$, or $s < t$ with s even. It remains to bound the cardinality of $W_s^{(i)}$ for $s = t$, and $i < s < t$ with s odd.

We consider two cases: Suppose first that $2i \le t$. Let $i < s < 2i$ with s odd (and so $s < t$). Let $v, v' \in W_s^{(i)}$ with $v \ne v'$. Since $v \not\approx_i v'$ we have that $|(1/v) - (1/v')| \ge q^{-2i+1}$ and so $|v - v'| \ge q^{2(s-i)+1}$. Furthermore, since $v, v' \in G$ and G is a group which contains only polynomials of odd degree (excluding those of degree t) we have that $\deg(v - v')$ is odd. We now apply Lemma 4 with $b = s$ and $a = 2(s-i)+1$ to deduce that $\#(W_s^{(i)}) \le (q-1)q^{(2i-s-1)/2}$. Writing $W_{\ge 2i}$ for $\cup_{s \ge 2i} W_s^{(i)}$ we see that if $W_{\ge 2i}$ contains two distinct members v and v' of degrees m and n respectively with $m \ge n \ge 2i$ then $q^m \ge |v - v'| \ge q^{-2i+m+n+1} \ge q^{m+1}$ which is a contradiction. Thus $\#(W_{\ge 2i}) \le 1$. It is a simple exercise in summing geometric series to then show that $\#(W^{(i)}) = \sum_{s>i} \#(W_s^{(i)}) = \sum_{i<s<2i, s\, odd} \#(W_s^{(i)}) + \#(W_{\ge 2i}) \le \sum_{i<s<2i, s\, odd} (q-1)q^{(2i-s-1)/2} + 1 = q^{\lfloor i/2 \rfloor}$.

Suppose now that $2i > t$. For $i < s \le t-1 < 2i$ and s odd one may show as before that $\#(W_s^{(i)}) \le (q-1)q^{(2i-s-1)/2}$. Similarly we may appeal to Lemma 4 to show that $\#(W_t^{(i)}) \le q^{(2i-t)/2}$. (Recall that $\#(G_t/G_{t-1}) = 2$ and so $n_t(W_t^{(i)}) = 1$ in Lemma 4 in this case.) Once again summing over s one concludes that $\#(W^{(i)}) = \sum_{i<s\le t-1} \#(W_s^{(i)}) + \#(W_t^{(i)}) \le \sum_{i<s\le t-1, s\, odd} (q-1)q^{(2i-s-1)/2} + q^{(2i-t)/2} = q^{\lfloor i/2 \rfloor}$.

To show that $w_i = q^{\lfloor i/2 \rfloor}$ one must first prove that the bounds on the cardinalities of the sets $W_s^{(i)}$ discussed above can actually be met. For each i $(1 \le i \le t-1)$, and each suitable s, we show that one may construct a set $W_s^{(i)}$, of polynomials of degree s in G which lie in distinct $\approx_i$-equivalence classes, whose cardinality meets the appropriate bound. (For each i, we also define a set $W_{\geq 2i}$ which we need in the case $2i \leq t$.) We then take suitable unions of these sets to give for each required i a set $W^{(i)}$, of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes, such that $\#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$.

For s even or s greater than t, we define $W_s^{(i)} = \emptyset$. In the case $2i \leq t$ we define $W_{\geq 2i} = \{f\}$ where f is any polynomial in G with degree at least $2i$. The main cases to consider are s odd with $i < s < t$, and $s = t$. In the former case, one must show that for each $i\,(1 \leq i \leq t-1)$ there exists a set $W_s^{(i)}\,(i < s \leq \min\{2i-1, t\}$, s odd) of $(q-1)q^{(2i-s-1)/2}$ polynomials in G which have degree s such that distinct elements lie in different $\approx_i$-equivalence classes. That is to say: $v, v' \in W_s^{(i)}$ with $v \neq v' \Rightarrow |v - v'| \geq q^{2(s-i)+1}$. We construct such a set as follows: For each positive m which is odd and less than t, choose polynomials $f_{m_0}, f_{m_1}, \ldots, f_{m_{q-1}}$ such that the images of the f_{m_i} under the natural homomorphism $G_m \to G_m/G_{m-2}$ are distinct. (One may do this since G is a maximal solution group.) We may assume that $\deg f_{m_i} = m$ for $1 \leq i \leq q-1$. Let the set $W_s^{(i)}$ be given by

$$W_s^{(i)} = \{f_{s_i} + \sum_{\substack{2(s-i)+1 \leq m \leq s-2 \\ m\, odd}} f_{m_{j_m}} \mid 1 \leq i \leq q-1;\ \text{for each } m, 0 \leq j_m \leq q-1\}.$$

It is easy to verify that $W_s^{(i)}$ meets our requirements.

The case $s = t$ is similar. It is easily verified that for each $i\,(1 \leq i \leq t-1)$ the set $W_t^{(i)}$ constructed as follows has cardinality $q^{(2i-t)/2}$, and if $v, v' \in W_t^{(i)}$ with $v \neq v'$ then $|v - v'| \geq q^{2(t-i)+1}$, and so distinct members lie in different $\approx_i$-equivalence classes: Let f_{t_0} and f_{t_1} be elements in G_t with distinct images under the natural homomorphism $G_t \to G_t/G_{t-1}$, and $f_{m_0}, f_{m_1}, \ldots, f_{m_{q-1}}$ (m odd and less than t) be as in the preceding paragraph. (Such elements exist since G is maximal.) We may assume $\deg f_{t_1} = t$. Let $W_t^{(i)}$ be given by

$$W_t^{(i)} = \{f_{t_1} + \sum_{\substack{2(t-i)+1 \leq m \leq t-1 \\ m\, odd}} f_{m_{j_m}} \mid \text{For each } m,\ 0 \leq j_m \leq q-1\}.$$

Finally, for each $i\,(1 \leq i \leq t-1)$ we define a set $W^{(i)}$, of polynomials of degree greater than i which lie in distinct $\approx_i$-equivalence classes, with

$\#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$: For $2i \leq t$ let $W^{(i)} = \cup_{i<s<2i} W_s^{(i)} \cup W_{\geq 2i}$ and for $2i > t$ let $W^{(i)} = \cup_{i<s\leq t-1} W_s^{(i)} \cup W_t^{(i)}$. From the construction of the sets $W_s^{(i)}$ we know that $W^{(i)}$ will in both cases have the appropriate cardinality. We need to show that distinct polynomials in $W^{(i)}$ lie in different $\approx_i$-equivalence classes. Let $v, v' \in W^{(i)}$ with $\deg v = s$, $\deg v' = s'$, and $v \neq v'$. Now $W^{(i)}$ can contain at most one polynomial of degree greater than $2i$. So $s, s' \leq 2i$ and $v \in W_s^{(i)}$, $v' \in W_{s'}^{(i)}$. If $s = s'$ then $v \not\approx_i v'$ by our previous observations on the set $W_s^{(i)} (= W_{s'}^{(i)})$. If $s \neq s'$ then $|(1/v) - (1/v')| = q^{-\min\{s,s'\}} \geq q^{-2i+1}$ since $\min\{s, s'\}$ is odd. Hence $v \not\approx_i v'$ in this case. Thus $w_i = \#(W^{(i)}) = q^{\lfloor i/2 \rfloor}$ which completes the proof.

□

Recall that we say that two sets of polynomials are equivalent if any polynomial of degree at least 1 which lies in one, lies in the other.

Lemma 11 *Let $u \in \mathbb{F}_q[x]$ have positive even degree and* $\operatorname{char} \mathbb{F}_q = 2$. *If H is a solution set for u which is equivalent to a maximal solution group for u then the cardinality of $CF(H)/\sim_{2n-1}$ is q^n. If H is a solution set for u which is not equivalent to a maximal solution group then the cardinality of $CF(H)/\sim_{2n-1}$ is strictly less than q^n for sufficiently large n.*

Proof: Let $G = G(u)$ denote the full solution group for u and let H be a solution set for u. Denote the degree enumerator and deficiency polynomials for G and H by $f_G(z)$, $g_G(z)$ and $f_H(z)$, $g_H(z)$ respectively. Suppose that H is equivalent to a maximal solution group for u. Then in this case G must be maximal and from Lemmas 9 and 10, the rational function $g_G(z)/(1 - f_G(z))$ is $(1 - qz)^{-1}$. But H is equivalent to G and so $g_H(z)/(1 - f_H(z)) = g_G(z)/(1 - f_G(z))$. So by Proposition 5, the cardinality of $CF(H)/\sim_{2n-1}$ is q^n.

We now consider the second case in which H is not equivalent to a maximal solution group. The coefficients of $f_H(z)$ are positive real numbers and are bounded by those of $f_G(z)$; thus $f_H(z) \leq f_G(z)$ for all positive real z. We claim that $f_H(1/q) < 1$: In the case that G is maximal we have that $f_G(1/q) = 1$ and so $f_H(1/q) < 1$ since at least one coefficient of $f_H(z)$ is strictly smaller than the corresponding coefficient of $f_G(z)$ (here H is not equivalent to G). If G is not maximal then it is not difficult to see that $f_G(1/q) < 1$. Since $f_H(1/q) \leq f_G(1/q)$ our claim is also true in this case.

Now let β be the root of $1 - f_H(z)$ with smallest complex modulus. If $\|\beta\| \leq 1/q$ then $\|1 - f_H(\beta)\| \geq 1 - f_H(\|\beta\|) \geq 1 - f_H(1/q) > 0$ (the penultimate inequality holds because f_H is an increasing function on the positive reals). Hence $\|\beta\| > 1/q$. Letting $S = H$ in Proposition 5 and choosing ε in the second part of the proposition so that $\|\beta\| - \varepsilon > 1/q$ yields the second statement.

□

We may now state the main result of this section.

Lemma 12 *Let $u \in \mathbb{F}_q[x]$ have positive even degree and* $\operatorname{char} \mathbb{F}_q = 2$. *Then $I_u = CF(S)$ if and only if S is equivalent to a maximal solution group for u.*

Proof: ($\Leftarrow$) Suppose that S is equivalent to a maximal solution group for u. Let $g, g' \in D_u$ with $\phi(g) = f$ and $\phi(g') = f'$ where $f, f' \in I_u$. Subtracting the relevant equations we find that

$$(f - f')^2 + u(f - f') = x(g - g')^2$$

and so $|g - g'|^2 = q^{t-1}|f - f'|$. From this it follows that

$$g \sim_{n-(t/2)} g' \Leftrightarrow f \sim_{2n-1} f' \tag{1}$$

where $\deg u = t$.

Thus $\#(I_u/\sim_{2n-1}) = \#(D_u/\sim_{n-(t/2)}) = q^n$ (the first equality holds because of (1) and the final one comes directly from the definition of D_u). From Lemma 11, $\#(CF(S)/\sim_{2n-1}) = q^n$ since S is a equivalent to a maximal solution group, and so $\#(CF(S)/\sim_{2n-1}) = \#(I_u/\sim_{2n-1})$ for each n. Furthermore $CF(S) \subseteq I_u$ by Lemma 7. Suppose that $CF(S) \neq I_u$. Let $f \in I_u$ with $f \notin CF(S)$. In particular, for some m we have that $f \not\sim_{2m-1} f'$ for all $f' \in CF(S)$. Since $CF(S) \subseteq I_u$ it follows that $\#(I_u/\sim_{2m-1}) > \#(CF(S)/\sim_{2m-1})$, which is a contradiction. Thus $CF(S) = I_u$.

($\Rightarrow$) Suppose that S is not equivalent to a maximal solution group for u. If S is not equivalent to a solution set for u then the contrapositive of

($\Rightarrow$) in Lemma 7 shows that $CF(S) \not\subseteq I_u$. So suppose that S is equivalent to a solution set for u but is not equivalent to a maximal solution group. Then by Lemma 11 the cardinality of $CF(S)/\sim_{2n-1}$ is strictly less than q^n for sufficiently large n. But if $CF(S) = I_u$ then we must have that $\#(CF(S)/\sim_{2n-1}) = \#(I_u/\sim_{2n-1}) = q^n$ for all n. Therefore $CF(S) \neq I_u$ as required.

$\square$

4.3 The case $\deg u$ odd

The case $\deg u$ odd can be treated in a similar way to $\deg u$ even, modulo a few changes which we describe in this section.

The full solution group $G(u)$ of a polynomial u of odd degree t is defined in exactly the same way and any subset of this group is called a solution set for u. The full solution group $G(u)$ is said to be maximal if its degree enumerator $f(z)$ is of the form

$$f(z) \quad = \quad \sum_{\substack{1 \leq i \leq t-1 \\ i \; even}} (q-1)q^{i/2} z^i + q^{(t+1)/2} z^t.$$

In this case we have the factorisation

$$1 - f(z) \quad = \quad (1 - qz)(1 + \sum_{\substack{1 \leq i \leq t-2 \\ i \; odd}} q^{(i+1)/2}(z^i + z^{i+1})).$$

For any finite subset S of $\mathbb{F}_q[x]$, recall (from the discussion following Proposition 5) that one may define the new deficiency polynomial $\hat{g}_S(z) = \sum_{i \geq 0} \hat{w}_i z^i$. We then have that the cardinality of $CF(S)/\sim_{2n}$ equals the coefficient of z^n in $\hat{g}_S(z)/(1 - f_S(z))$, where $f_S(z)$ is the degree enumerator of S. Examining the proof of Lemma 12, we see that to establish an odd case version of the lemma we need to show the following: if $G(u)$ is a maximal solution group for u then $\#(CF(G(u))/\sim_{2n}) = q^n$, and if H is any solution set which is not equivalent to a maximal solution group then $\#(CF(H)/\sim_{2n}) < q^n$ for sufficiently large n. Once again, the latter is straightforward and follows from the fact that the complex modulus of the smallest root of $1 - f_H(z)$ in the case that H is a solution set for u which is not equivalent to a maximal solution group is strictly greater than $1/q$. To prove the former we must establish the form of the new deficiency polynomial $\hat{g}(z)$ of a maximal solution group $G(u)$. We must show that it is equal to the cofactor of $1 - qz$ in the above factorisation of $1 - f(z)$. Fortunately, we can use Lemma 10 to do this: Observe first that if $G(u)$ is a maximal solution group for u where $\deg u$ is odd, then $xG(u)$ is a maximal solution group for xu, which has even degree. Now suppose that $W \subseteq G(u)$ is a set of polynomials of degree greater than i which lie in distinct $\simeq_i$-equivalence classes. Then it is easily seen that $xW \subseteq xG(u)$ is a set of polynomials of degree greater than $i+1$ which lie in distinct $\approx_{i+1}$-equivalence classes. One may deduce (with a little work) from this observation and Lemma 10 that for i with $1 \leq i \leq t-1$ the coefficient of z^i in $\hat{g}(z)$ is $q^{(i+1)/2}$ if i is odd, and $q^{i/2}$ if i is even. Thus $\hat{g}(z)$ has the required form.

Lemma 12 together with the odd case version of the lemma whose proof we have just outlined together establish Theorem 1.

4.4 Polynomials with maximal solution groups

In this section, we will be concerned with finding all polynomials whose full solution groups are maximal. We shall see that they do not exist for fields with more than 4 elements; however, we are able to give a complete description in the case that the field has 2 or 4 elements.

We begin with a result which implies that in the search for polynomials with maximal solution groups we may restrict our attention to the fields with two elements and four elements.

Proposition 13 *Let* $u \in \mathbb{F}_q[x]$ *with* $\deg u \geq 1$*, where* $\operatorname{char} \mathbb{F}_q = 2$ *and* $q \neq 2$ *or* 4*. The full solution group for* u *is not maximal.*

Proof: Let $u \in \mathbb{F}_q[x]$ with $\deg u \geq 1$ and $\operatorname{char} \mathbb{F}_q = 2$. Observe that if $G(u)$ is a maximal solution group for u where $\deg u$ is odd, then $xG(u) = \{xv \mid v \in G(u)\}$ is a maximal solution group for xu. We may therefore assume that u has even degree at least 2. Suppose that $G(u)$

is maximal; so it meets the bounds imposed by Lemma 8. In particular $\#(V_1) = \#(G_1) - \#(G_{-1}) = q-1$. Let $u = \sum_{0 \le i \le t} u_i x^i$ and $v = a + bx \in V_1$. Then the polynomial $v^2 + uv$ contains only odd powers of x. Thus the coefficients of x^0 and x^2 in $v^2 + uv$, which are $a^2 + au_0$ and $b^2 + bu_1 + au_2$ respectively, are both 0. We conclude that $a = 0$ or u_0. If $a = 0$ then $b = u_1$, since we must assume that $b \neq 0$. When $a = u_0$, b can take at most 2 values. Hence $\#(V_1) \le 3$. Thus $q - 1 = \#(V_1) \le 3$, which completes the proof.

□

We now determine all polynomials over the field with four elements which have maximal solution groups.

Proposition 14 *Let $u \in \mathbb{F}_4[x]$ with $\deg u \ge 1$. Then the full solution group for u is maximal if and only if $u = u_0 + u_1 x + u_2 x^2$ where $u_0 u_2 = u_1^2 \neq 0$.*

Proof: We first consider the case $\deg u = 2$ and so $u = u_0 + u_1 x + u_2 x^2$. Then $G(u)$ is maximal if and only if $\#(V_1) = 4 - 1 = 3$ and $\#(V_2) = 4$. If $\#(V_1) = 3$ then since $u \in V_2$ and $u + V_1 \subseteq V_2$ we have that $\#(V_2) = 4$. Thus $G(u)$ is maximal if and only if $\#(V_1) = 3$. We have seen from the proof of Proposition 13 that this is true precisely when $u_0 \neq 0$ (this ensures that the a in Proposition 13 can take two distinct values) and there are two elements b_1 and b_2 in $\mathbb{F}_4$ such that $b_i^2 + u_1 b_i + u_0 u_2 = 0$ $(i = 1, 2)$ (this ensures the non-zero value of a will yield two distinct choices for b). Observe that $u_1 \neq 0$ in this case. Making the substitution $b_i = u_1 c_i \in \mathbb{F}_4$ and dividing by u_1^2 we see that $\mathrm{Tr}(c_i) := c_i^2 + c_i = u_0 u_2 / u_1^2$. If $u_0 u_2 / u_1^2 \in \mathbb{F}_2$ there are two distinct such c_i, and otherwise there are none. We have therefore shown that any polynomial of degree 2 with a maximal solution group must be of the form described in the proposition. If $\deg u = 1$ and $G(u)$ is maximal then xu has a maximal solution group $G(xu) = xG(u)$. But xu has a zero constant term. This contradicts our description of polynomials of degree 2 with maximal solution groups. Thus there are no polynomials of degree 1 with maximal solution groups.

Suppose now that $\deg u > 2$ with $u = \sum_{0 \le i \le t} u_i x^i$. Once again, we may assume that $\deg u$ is even. Let $G(u)$ be a maximal solution group for u. Then $G(u)$ must contain $(q-1)q = 12$ polynomials of degree 3. Let

$v_0 + v_1x + v_2x^2 + v_3x^3 \in V_3$. So $v_3 \neq 0$. Then the coefficients of x^0, x^2, x^4, x^6 in $v^2 + uv$ are 0. Therefore

$$\begin{aligned} v_0^2 + u_0v_0 &= 0 \\ v_1^2 + u_0v_2 + u_1v_1 + u_2v_0 &= 0 \\ v_2^2 + u_1v_3 + u_2v_2 + u_3v_1 + u_4v_0 &= 0 \\ v_3^2 + u_3v_3 + u_4v_2 &= 0 \end{aligned}$$

One may use ad hoc arguments to show that the above system of equations has at most 8 solutions (v_0, v_1, v_2, v_3) with $v_3 \neq 0$, for any choice of u_i ($0 \leq i \leq 4$). Therefore $G(u)$ cannot be maximal. This contradiction completes the proof.

□

The above lemma gives a family of 9 polynomials u of degree 2 over $\mathbb{F}_4$ with $I_u = CF(G(u))$. More explicitly, if $u = u_0 + u_1x + u_2x^2 \in \mathbb{F}_4[x]$ where $u_0u_2 = u_1^2 \neq 0$, then $G(u)$ is the additive group generated by the polynomials $u_1x, u_0 + \alpha u_1x, u_0 + (1+\alpha)u_1x$, and u. Here $\alpha \in \mathbb{F}_4$ with $\alpha \neq 0, 1$.

We conclude by considering the $\mathbb{F}_2$ case.

Proposition 15 *Let $u \in \mathbb{F}_2[x]$ with $\deg u > 6$. The full solution group of u is not maximal.*

Proof: Once again it is enough to prove the proposition for u a polynomial of even degree t with $t \geq 8$. So suppose that u is such a polynomial and $G(u)$ is maximal. Then either x or $x+1$ lies in $G(u)$ and also one of x^3, x^3+1, x^3+x^2 or x^3+x^2+1 must lie in $G(u)$.

Suppose that $x \in G(u)$. Then $u = x + \sum_{i \in M} x^i + x^t$ where $M \subseteq \{2, 4, \ldots, t-2\}$. Now $x^3 \notin G(u)$ as $x^6 + ux^3$ contains the even power x^4. Also $x^3 + 1 \notin G(u)$ as $x^6 + 1 + (x^3+1)u$ contains the term x^t (since $t > 6$). Similarly, if $v = x^3 + x^2$ or $x^3 + x^2 + 1$ then $v \notin G(u)$ since $v^2 + uv$ contains the even power x^{t+2} (since $t + 2 > 6$).

Hence $x + 1 \in G(u)$. So u must include the term x^{t-1}. Also observe that $(x+1)u$ consists of 1, x^2 and odd powers of x. If $v = x^3$ or $x^3 + 1$ then $v \notin G(u)$ since $v^2 + uv$ contains the even power x^{t+2}. If $v = x^3 + x^2$ then $x^6 + x^4 + x^2(x+1)u$ contains the term x^6 by our previous observation and

The polynomial u	The maximal solution group $G(u)$
$x+1$	$\langle 1, u\rangle$
x^2+x	$\langle x, u\rangle$
x^2+1	$\langle x+1, u\rangle$
x^2+x+1	$\langle x, u\rangle$
x^3+1	$\langle 1, x^2+x+1, u\rangle$
x^4+x	$\langle x, x^3+x^2+x, u\rangle$
x^4+x^3+x+1	$\langle x+1, x^3+1, u\rangle$
$x^4+x^3+x^2+1$	$\langle x+1, x^3+x+1, u\rangle$
x^4+x^2+x+1	$\langle x, x^3+x^2+1, u\rangle$
$x^6+x^5+x^2+1$	$\langle x+1, x^3+x^2+1, x^5+x+1, u\rangle$
x^6+x^4+x+1	$\langle x, x^3+1, x^5+x^4+1, u\rangle$

Table 1: Polynomials with maximal full solution groups in $\mathbb{F}_2[x]$

so $v \notin G(u)$. Finally, $x^3+x^2+1 \notin G(u)$ as $x^6+x^4+1+x^2(x+1)u+u$ contains the even power x^t (since $t > 6$). This contradiction completes the proof.

□

We list all polynomials $u \in \mathbb{F}_2[x]$ whose full solution groups are maximal in Table 1 along with (the generators of) their full solution groups.

5 Corollaries to Theorem 1

In this section, we discuss some applications of Theorem 1 and the results which follow it. The first is to the problem of constructing algebraic Laurent series with partial quotients of bounded degree, and the second to the study of sequences over fields.

5.1 Algebraic Laurent series with bounded partial quotients

There is a well-known conjecture in number theory which asserts that the partial quotients of the continued fraction expansion of an algebraic real number of degree at least 3 are unbounded; however, almost nothing is known about the continued fractions of such numbers. The situation over fields of Laurent series in positive characteristic is somewhat different; in particular, in recent years several explicit expansions of algebraic Laurent series which have bounded partial quotients have been given. The first and simplest result along these lines is that over the binary field, there exist algebraic Laurent series of every even degree, whose partial quotients are all linear polynomials [2]. We prove a similar result for the field of four elements.

Corollary 16 *Let $d \in \mathbb{N}$. There exists an element of L_4 with linear or quadratic partial quotients which is algebraic of degree d or $2d$ over $\mathbb{F}_4(x)$.*

Proof: Let u be a polynomial over $\mathbb{F}_4$ of degree 2 whose full solution group $G(u)$ is maximal (such polynomials exist by Proposition 14). Let $g \in L_4$ be algebraic of degree d over $\mathbb{F}_4(x)$ with $|g| \leq 1 = q^{\lfloor 2/2 \rfloor - 1}$. Now g^2 has either degree d or possibly, if d is even, degree $d/2$ over $\mathbb{F}_4(x)$. We show that the latter cannot occur. For suppose g^2 has degree $d/2$ with minimum polynomial $h(X)$ where $\deg_X h = d/2$. Then g is a repeated root of $h(X^2)$ and $\deg_X h(X^2) = d$. Since g has degree d, $h(X^2)$ must be the minimum polynomial of g, and so g is not separable. But every finite extension of $\mathbb{F}_4(x)$ in L_4 is separable (see the proof of "Theorem 8" in [1]). Hence g^2 is algebraic of degree d. So the unique element $f \in CF(G(u)) \subseteq P_4$ for which $f^2 + uf + (1 + xg^2) = 0$ has degree d or $2d$. The partial quotients of the continued fraction of f belong to $G(u)$ and so have degree 1 or 2. This completes the proof.

□

5.2 An application to sequences

Let $s = \{s_i\}_{i\ge 1}$ be a sequence over the field $\mathbb{F}_q$. One measure of the predictability of a sequence which is of interest in stream cipher theory, a part of cryptography, is its linear complexity profile. In this section, we discuss sequences which have prescribed linear complexity profiles, and mention how this relates to rational functions whose continued fractions have partial quotients of prescribed degrees.

The *linear complexity profile* of a sequence $s = \{s_i\}_{i\ge 1}$ over $\mathbb{F}_q$ may be defined as follows: For $n \ge 1$ let $l_n(s)$ denote the length of the shortest linear recurrence satisfied by the truncated sequence $\{s_i\}_{1\le i\le n}$. (The least m such that there exists $f_i \in \mathbb{F}_q\,(0 \le i \le m)$ which are not all zero, with $\sum_{0\le i\le m} f_i s_{k+i} = 0$ for all $1 \le k \le n-m$.) The linear complexity profile of s is the sequence $\{l_n(s)\}_{n\ge 1}$. Observing that $l_n(s) \le l_{n+1}(s)\,(n \ge 1)$, we define the *jumps profile* of s to be the subsequence of non-zero terms in the (non-negative) sequence $l_1(s), l_2(s) - l_1(s), l_3(s) - l_2(s), \ldots$. The set of positive integers which appear in the jumps profile are called the *jumps* of s, and a linear complexity profile with jumps of size 1 is called *perfect*. Wang's modification [12] of Niederreiter's result [8] on the relation between continued fractions of Laurent series and sequences asserts that the jumps profile of a sequence $\{s_i\}_{i\ge 1}$ is $\{\deg a_i\}_{i\ge 1}$ where $\sum_{i\ge 1} s_i x^{-i} = [\,0; a_1, a_2, \ldots]$.

Each polynomial in Table 1 gives us a different family of binary sequences with particular linear complexity profiles which satisfy simple linear recurrences. For example, taking $u = x + 1$ gives us the well-known result that a binary sequence $\{s_i\}_{i\ge 1}$ has a perfect linear complexity profile if and only if it satisfies

$$\begin{aligned}
&s_1 = 1,\\
&s_i + s_{2i} + s_{2i+1} = 0 \quad \text{for } i \ge 1.
\end{aligned}$$

It is remarkable that one may characterise these sequences in such a simple way, and this characterisation has been applied to the following problem on rational functions over $\mathbb{F}_2$ whose continued fractions have partial quotients of small degree [3, 4, 6, 7]: Determine for which polynomials g over $\mathbb{F}_2$, there exists a coprime polynomial f over $\mathbb{F}_2$ of degree less than g, such that all the partial quotients of the continued fraction of f/g have degree 1. If a suitable polynomial f exists for some g, how many such f are there? The latter question has been settled although the former remains open.

For $u = x^3 + 1$ we get that a binary sequence which satisfies

$$\begin{aligned} &s_1 = 0,\ s_3 = 1, \\ &s_i + s_{2i} + s_{2i+3} = 0 \quad \text{for } i \geq 1, \end{aligned}$$

has a linear complexity profile with jumps of size 2 and 3. The converse is not true in that there exist sequences whose linear complexity profiles have jumps of size 2 and 3 but which do not satisfy the above recurrence. However, it is easy to classify exactly which sequences do (namely those whose associated continued fraction has partial quotients which are from the full solution group of $x^3 + 1$). We obtain similar information for every other polynomial in the table.

We do not get such neat linear recurrences for sequences over $\mathbb{F}_4$; however, we have the following "$\mathbb{F}_2$-linear" result.

Corollary 17 *Let $u_0, u_1, u_2 \in \mathbb{F}_4$ with $u_0 u_2 = u_1^2 \neq 0$. Then a sequence $\{s_i\}_{i\geq 1}$ over $\mathbb{F}_4$ which satisfies*

$$\begin{aligned} &u_2 s_2 + u_1 s_1 + 1 = 0, \\ &u_2 s_{2i+2} + u_1 s_{2i+1} + u_0 s_{2i} + s_i^2 = 0 \quad \textit{for } i \geq 1, \end{aligned}$$

has a linear complexity profile with jumps of size 1 *and* 2.

Proof: It is easily seen that if $\{s_i\}_{i\geq 1}$ satisfies the recurrence relations then the Laurent series $f = \sum_{i\geq 1} s_i x^{-i}$ will satisfy $f^2 + uf + (1 + xg^2)$ for some $g \in L_4$. Here $u = u_0 + u_1 x + u_2 x^2$. (Compare the recurrence relations with those in the proof of Lemma 6.) The conditions on the coefficients of u ensure that $I_u = CF(G(u))$ (by Theorem 1 and Proposition 14) and so $f \in CF(G(u))$. Thus the partial quotients in the continued fraction of f have degree 1 or 2 and so by the theorem of Niederreiter and Wang we know that the sequence $\{s_i\}_{i\geq 1}$ must have a jumps profile which consists solely of ones and twos.

$\square$

It is conceivable that this corollary could be used to prove results for rational functions over the field $\mathbb{F}_4$ whose continued fractions have partial quotients of small degree.

References

[1] L.E. Baum and M.M. Sweet, *Continued fractions of algebraic power series in characteristic* 2, Ann. of Math. 103 (1976), 593-610.

[2] L.E. Baum and M.M. Sweet, *Badly approximable power series in characteristic* 2, Ann. of Math. 105 (1977), 573-580.

[3] S.R. Blackburn, *Orthogonal sequences of polynomials over arbitrary fields*, J. Number Theory 68 (1998), 99-111.

[4] A.G.B. Lauder, *Polynomials with odd orthogonal multiplicity*, Finite Fields and Their Applications 4 No. 4 (1998), 453-464.

[5] A.G.B. Lauder, *Continued fractions and sequences*, Ph.D. Thesis, University of London, 1999.

[6] J.P. Mesirov and M.M. Sweet, *Continued fraction expansions of rational expressions with irreducible denominators in characteristic* 2, J. Number Theory 28 (1987), 144-148.

[7] H. Niederreiter, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatsh. Math 103 (1987), 269-288.

[8] H. Niederreiter, *Sequences with almost perfect linear complexity profiles*, in: Advances in Cryptology - Eurocrypt '87, D. Chaum and W.L. Price (eds), Lecture Notes in Computer Science 304, Springer, 1988, 37-51.

[9] A.M. Odlyzko, *Asymptotic enumeration methods*, in: Handbook of Combinatorics, vol. 2, R.L. Graham, M. Groetschel, L. Lovasz (eds), Elsevier Science, 1995, 1063-1229.

[10] A.J. van der Poorten, J. Shallit, *Folded continued fractions*, J. Number Theory 40 (1992), 237-250.

[11] A.M. Rockett and P. Szüsz, *Continued Fractions*, World Scientific Publishing, 1992.

[12] M. Wang, *Linear complexity profiles and continued fractions*, in: Advances in Cryptology - Eurocrypt '89, J-J. Quisquater and J. Vandewalle (eds), Lecture Notes in Computer Science 434, Springer, 1989, 571-585.

[13] H.S. Wilf, *Generatingfunctionology*, 2nd edn, Academic Press, 1994.

Royal Holloway
University of London
Egham, Surrey TW20 0EX
United Kingdom
E-mail: a.lauder@rhbnc.ac.uk