# Polynomials with Odd Orthogonal Multiplicity

Alan G.B. Lauder*
Department of Mathematics,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, United Kingdom

June 23, 1998

*The author is an EPSRC CASE student sponsored by the Vodafone Group. This paper has been accepted for publication in *Finite Fields and Their Applications*.

**Abstract**

Let the *orthogonal multiplicity* of a monic polynomial $g$ over a field $\mathbb{F}$ be the number of polynomials $f$ over $\mathbb{F}$, coprime to $g$ and of degree less than that of $g$, such that all the partial quotients of the continued fraction expansion of $f/g$ are of degree 1. Polynomials with positive orthogonal multiplicity arise in stream cipher theory, part of cryptography, as the minimal polynomials of the initial segments of sequences which have perfect linear complexity profiles. This paper focuses on polynomials which have odd orthogonal multiplicity; such polynomials are characterized and a lower bound on their orthogonal multiplicity is given. A special case of a conjecture on rational functions over the finite field of two elements with partial quotients of degree 1 or 2 in their continued fraction expansion is also proved.

## 1 Introduction

If $f$ and $g$ are polynomials over an arbitrary field $\mathbb{F}$ with $\gcd(f, g) = 1$ and $deg\, g \geq 1$, then the rational function $f/g$ has a unique continued fraction expansion

$$a_0 + 1/(a_1 + 1/(a_2 + \ldots + 1/a_m))$$

where $a_i \in \mathbb{F}[x]$ for $0 \leq i \leq m$ and $deg\, a_i \geq 1$ for $1 \leq i \leq m$. We write the above continued fraction as $[\, a_0\, ; a_1, a_2, \ldots, a_m\, ]$ and define

$$K\left(\frac{f}{g}\right) = \max_{1 \leq i \leq m} deg\, a_i.$$

For a monic $g \in \mathbb{F}[x]$ with $deg\, g = n \geq 1$, let $m(g)$ be the cardinality of the set

$$M_g = \{f/g \in \mathbb{F}(x) \mid deg\, f < n,\ \gcd(f, g) = 1,\ \text{and } K(f/g) = 1\}.$$

We call $m(g)$ the *orthogonal multiplicity* of $g$, or when there is no possibility of confusion, simply the *multiplicity* of $g$. This appellation is motivated by the 'orthogonal sequences of polynomials' studied in classical analysis [11]: one may show that a monic polynomial has positive orthogonal multiplicity if and only if it occurs as a term in some 'orthogonal sequence of polynomials' [1].

We will be concerned primarily with polynomials over finite fields which have positive orthogonal multiplicity; they arise in stream cipher theory, a sub-discipline of cryptography, as the minimal polynomials of the initial segments of sequences over finite fields with perfect linear complexity profiles. (The reader is referred to [8] in which Niederreiter establishes a connection between the linear complexity profiles of sequences and continued fractions over function fields.) More recently, Blackburn, and Cattell and Muzio have applied such polynomials to cellular automata theory [2, 3].

For an arbitrary field $\mathbb{F}$, it is of interest to ask exactly which polynomials over $\mathbb{F}$ have positive orthogonal multiplicity, and what can be said about their multiplicities. Some results in this direction (and in related areas [7, 9]) have already been established. In [1] Blackburn shows that if $\mathbb{F}$ has infinite order then every polynomial in $\mathbb{F}[x]$ has positive multiplicity; and if $\mathbb{F}_q$ denotes the finite field with $q$ elements [4] and $g \in \mathbb{F}_q[x]$ with $deg\, g = n$, then $g$ has positive multiplicity provided $\frac{1}{2}n(n+1) \leq q$. Blackburn conjectures that if $q \neq 2$ then every polynomial over $\mathbb{F}_q$ has positive multiplicity. The situation over $\mathbb{F}_2$ is somewhat different; in particular, there exist polynomials over $\mathbb{F}_2$ with multiplicity zero. However, Mesirov and Sweet [6] prove that all non-linear irreducible polynomials over $\mathbb{F}_2$ have multiplicity 2, and one may further show [1, 6] that if a polynomial $g$ over $\mathbb{F}_2$ has positive multiplicity then it has multiplicity $2^k$, where $k$ is the number of distinct non-linear irreducible factors of $g$.

In Section 3 of this paper we characterize polynomials which have odd orthogonal multiplicity and give a lower bound on the multiplicity of such polynomials. This bound is used in Section 4 to prove that if the characteristic of $\mathbb{F}_q$ is 2 and $q \neq 2$, then a polynomial over $\mathbb{F}_q$ has multiplicity $q-1$ if and only if it has degree 1; and an alternative characterization to that in Blackburn's paper [1] is given in Section 4 of polynomials over $\mathbb{F}_2$ of multiplicity 1. Section 4 also contains a proof of the following result: if $g \in$

$\mathbb{F}_2[x]$ splits into linear factors then there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f, g) = 1$ such that $K(f/g) \le 2$. This establishes a special case of a conjecture made by Mesirov and Sweet [6]. All of these results depend upon lemmas which are contained in Section 2.

The author would like to thank Simon Blackburn for his help and encouragement during the preparation of this paper.

## 2 Preliminaries

If $f/g = [\,0\,; a_1, a_2, \ldots, a_m\,]$ where $f$ and $g$ are polynomials over $\mathbb{F}$ and $deg\, g \ge 1$, then $kf/g = [\,0\,; k^{-1}a_1, ka_2, \ldots, k^{(-1)^m}a_m\,]$ for any $k \in \mathbb{F}^*$. Hence if $f/g \in M_g$ then $kf/g \in M_g$ for any $k \in \mathbb{F}^*$, and so the orthogonal multiplicity of a polynomial over a field $\mathbb{F}$ is a multiple of $|\mathbb{F}^*| = |\mathbb{F}| - 1$. Since we are interested solely in polynomials with odd multiplicity, we shall only be concerned with finite fields of characteristic 2. Throughout this section $\mathbb{F}_q$ will be a finite field of characteristic 2 (or more succinctly, *char* $\mathbb{F}_q = 2$).

### 2.1 Continued Fractions

Let $f/g$ be a rational function over the field $\mathbb{F}_q$ with $\gcd(f, g) = 1$ and $f/g = [\,a_0\,; a_1, a_2, \ldots, a_m\,]$. Define the polynomials $f_i$ and $g_i$ for $-1 \le i \le m$ by

$$\begin{array}{lll} f_{-1} = 1,\ f_0 = a_0, & f_i = a_i f_{i-1} + f_{i-2}\,, \text{ for } 1 \le i \le m, \\ g_{-1} = 0,\ g_0 = 1, & g_i = a_i g_{i-1} + g_{i-2}\,, \text{ for } 1 \le i \le m. \end{array} \tag{1}$$

For $0 \le i \le m$, the polynomials $a_i$ are called the *partial quotients* of $f/g$, and the rational function $f_i/g_i$ is called the $i^{th}$ *convergent* of $f/g$. It is easily shown that $f_i/g_i = [\,a_0\,; a_1, \ldots, a_i\,]$. One may write the above recurrences conveniently for $1 \le i \le m$ as

$$\begin{pmatrix} f_{i-1} & f_{i-2} \\ g_{i-1} & g_{i-2} \end{pmatrix} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_i & f_{i-1} \\ g_i & g_{i-1} \end{pmatrix},$$

and so

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_i & f_{i-1} \\ g_i & g_{i-1} \end{pmatrix}. \tag{2}$$

Following [10], we write

$$\begin{pmatrix} f_i & f_{i-1} \\ g_i & g_{i-1} \end{pmatrix} \leftrightarrow [\, a_0\, ; a_1, a_2, \ldots, a_i \,],$$

to indicate the correspondence between continued fractions and matrices of a particular form.

The above approach allows one to prove simple continued fraction identities with great ease. For example, taking the determinant of both sides of (2) gives us the well-known identity $f_i g_{i-1} - g_i f_{i-1} = (-1)^{i+1}$, or, as we are working in characteristic 2, $f_i g_{i-1} + g_i f_{i-1} = 1$. This implies that $\gcd(f_i, g_i) = 1$ and so the convergents are in reduced form.

The following lemma is central to the methods in this paper.

**Lemma 1** *Let* $\operatorname{char} \mathbb{F}_q = 2$ *and* $a \in \mathbb{F}_q[x]$. *For* $0 \le i \le m$, *let* $f_i/g_i$ *denote the* $i^{th}$ *convergent of the continued fraction* $[\, 0\, ; a_1, a_2, \ldots, a_m \,]$. *So* $f_m/g_m = [\, 0\, ; a_1, a_2, \ldots, a_m \,]$. *Then*

1. $g_{m-1}/g_m = [\, 0\, ; a_m, a_{m-1}, \ldots, a_1 \,]$.

2. $(f_m g_m + 1)/g_m^2 = [\, 0\, ; a_1, a_2, \ldots, a_{m-1}, a_m + 1, a_m + 1, a_{m-1}, \ldots, a_2, a_1 \,]$.

3. $(a f_m g_m + 1)/a g_m^2 = [\, 0\, ; a_1, a_2, \ldots, a_{m-1}, a_m, a, a_m, a_{m-1}, \ldots, a_2, a_1 \,]$.

The lemma may be deduced from results proved by Niederreiter in [7]; however, we give a simple proof which follows the approach taken by van der Poorten and Shallit in [10].

*Proof:* To prove Part 1, take the transpose of each side of (2). Putting $a_0 = 0$ and post-multiplying each side of the resulting identity by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gives us

$$\begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} g_i & f_i \\ g_{i-1} & f_{i-1} \end{pmatrix}. \tag{3}$$

Setting $i = m$ we get $g_m/g_{m-1} = [\,a_m\,; a_{m-1}, a_{m-2}, \ldots, a_1\,]$, and so $g_{m-1}/g_m = [\,0\,; a_m, a_{m-1}, \ldots, a_1\,]$.

We prove Part 2 by considering the matrix product

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m+1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m+1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\leftrightarrow [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m+1, a_m+1, a_{m-1}, \ldots, a_2, a_1\,].$$

Multiplying the first $m$ and the last $m-1$ matrices together using identities (2) and (3), with $i = m-1$, gives us

$$\begin{pmatrix} f_{m-1} & f_{m-2} \\ g_{m-1} & g_{m-2} \end{pmatrix} \begin{pmatrix} a_m+1 & 1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} g_{m-1} & f_{m-1} \\ g_{m-2} & f_{m-2} \end{pmatrix}.$$

We multiply these matrices using the fact that $f_{m-1}g_{m-2} + g_{m-1}f_{m-2} = 1$ to get

$$\begin{pmatrix} f_m g_m + 1 & f_m^2 \\ g_m^2 & f_m g_m + 1 \end{pmatrix},$$

and so $(f_m g_m{+}1)/g_m^2 = [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m{+}1, a_m{+}1, a_{m-1}, \ldots, a_2, a_1\,]$.

The steps in the proof of Part 3 are outlined below; in this case the identity $f_m g_{m-1} + g_m f_{m-1} = 1$ is used.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} f_m & f_{m-1} \\ g_m & g_{m-1} \end{pmatrix} \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} g_m & f_m \\ g_{m-1} & f_{m-1} \end{pmatrix} = \begin{pmatrix} af_m g_m + 1 & af_m^2 \\ ag_m^2 & af_m g_m + 1 \end{pmatrix}$$

$$\leftrightarrow [\,0\,; a_1, a_2, \ldots, a_{m-1}, a_m, a, a_m, a_{m-1}, \ldots, a_2, a_1\,].$$

□

Now, to facilitate the exposition, we introduce some new definitions and notation. Let $w = a_1 a_2 \ldots a_m$ be a word over the alphabet $\{a \in \mathbb{F}_q[x] \,|\, deg\, a \geq 1\}$. We let $\overrightarrow{w} = w$ and $\overleftarrow{w} = a_m a_{m-1} \ldots a_1$ and write $[\,w\,]$ to mean $[\,0\,; a_1, a_2, \ldots, a_m\,]$. If $\overrightarrow{w} = \overleftarrow{w}$ then we call $[\,w\,]$ a *symmetric* continued fraction. Define the mapping $\phi$ on the set of all words by $\phi : a_1 a_2 \ldots a_m \mapsto a_1 a_2 \ldots a_{m-1}(a_m + 1)$. Since $char\, \mathbb{F}_q = 2$, the map $\phi$ is an involution.

Let $g$ be a monic polynomial and suppose that $[\,w\,] \in M_g$, so each letter in the word $w$ is a polynomial of degree 1. It is easily seen, by considering the recurrence relations (1) that generate the convergents of $[\,w\,]$, that $m = deg\, g$. The following observation will be of use in the proof of Theorem 4.

**Observation:** If $[\,w\,] \in M_g$ is a symmetric continued fraction and $deg\, g$ is even then $w = \overrightarrow{v}\, \overleftarrow{v}$ for some word $v$, and if $deg\, g$ is odd then $w = \overrightarrow{v}\ a\ \overleftarrow{v}$ for some word $v$ and polynomial $a$ of degree 1.

We restate the results in Lemma 1 which are of greatest relevance to us in the following way.

**Lemma 2** *Let $\mathbb{F}_q$ be a finite field of characteristic 2.*

1. *If $g$ is a monic polynomial and $[\overrightarrow{w}] \in M_g$, then $[\overleftarrow{w}] \in M_g$.*

2. (i) *If $g$ is a monic polynomial and $[\overrightarrow{w}\overleftarrow{w}] \in M_g$, then $g = h^2$ for some monic polynomial $h$ and $[\overrightarrow{\phi(w)}] \in M_h$.*

   (ii) *If $h$ is a monic polynomial, $[\overrightarrow{w}] \in M_h$ and $g = h^2$, then $[\overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}] \in M_g$.*

3. (i) *If $g$ is a monic polynomial and $[\overrightarrow{w}\ a\ \overleftarrow{w}] \in M_g$ with $a = kb$, $b$ a monic polynomial of degree 1 and $k \in \mathbb{F}_q^*$, then $g = bh^2$ for some monic polynomial $h$ and $[\overrightarrow{w}] \in M_h$.*

   (ii) *If $h$ is a monic polynomial, $[\overrightarrow{w}] \in M_h$, and $g = bh^2$ where $b$ is a monic polynomial of degree 1, then $[\overrightarrow{w}\ a\ \overleftarrow{w}] \in M_g$ for any $a = kb$ where $k \in \mathbb{F}_q^*$.*

*Proof:* The lemma is essentially a rewording of the special case of Lemma 1 in which all the partial quotients $a_i\,(1 \leq i \leq m)$ of $f/g$ and the polynomial $a$ are of degree 1. We prove Part 3; the other parts are proved in a similar way.

*3(i)* Let $[\overrightarrow{w}\ a\ \overleftarrow{w}] \in M_g$ where $a = kb$ with $b$ a monic polynomial of degree 1 and $k \in \mathbb{F}_q^*$. Then there exists $f \in \mathbb{F}_q[x]$ with $f/g = [\overrightarrow{w}\ a\ \overleftarrow{w}]$. If we write $w = a_1a_2\ldots a_m$ where $deg\, a_i = 1\,(1 \leq i \leq m)$, and let $r_m/s_m$ denote the $m^{th}$ convergent of the continued fraction $[w]$, then by Lemma 1 Part 3, $(ar_ms_m + 1)/as_m^2 = [\overrightarrow{w}\ a\ \overleftarrow{w}]$. Hence $(ar_ms_m + 1)/as_m^2 = f/g$. Let $as_m^2 = lbh^2$ where $h$ is monic and $l \in \mathbb{F}_q^*$. Then $l^{-1}(ar_ms_m + 1)/bh^2 = f/g$

with $\gcd(l^{-1}(ar_m s_m+1), bh^2) = \gcd(ar_m s_m+1, as_m^2) = 1$. Since $\gcd(f,g) = 1$ and both $bh^2$ and $g$ are monic, we have that $g = bh^2$. Finally, $[\overrightarrow{w}] \in M_h$ since $\sqrt{kl^{-1}}r_m/h = [\overrightarrow{w}]$ and each letter in the word $w$ is a polynomial of degree 1.

*3(ii)* Let $[\overrightarrow{w}] \in M_h$ where $h$ is monic, and let $g = bh^2$ where $b$ is monic of degree 1. Let $a = kb$ for some $k \in \mathbb{F}_q^*$. If we write $w = a_1 a_2 \dots a_m$ where $deg\, a_i = 1\,(1 \leq i \leq m)$, and let $r_m/s_m$ denote the $m^{th}$ convergent of the continued fraction $[\overrightarrow{w}]$, then by Lemma 1 Part 3, $(ar_m s_m + 1)/as_m^2 = [\overrightarrow{w}\ \ a\ \ \overleftarrow{w}]$. Now $s_m = lh$ for some $l \in \mathbb{F}_q^*$, and so $as_m^2 = kl^2bh^2$. Thus $k^{-1}l^{-2}(ar_m s_m+1)/bh^2 = (ar_m s_m+1)/as_m^2$ and, moreover, $\gcd(k^{-1}l^{-2}(ar_m s_m+1), bh^2) = \gcd(ar_m s_m+1, as_m^2) = 1$. Since $g = bh^2$ and all the letters in the word $\overrightarrow{w}\ a\ \overleftarrow{w}$ are polynomials of degree 1, we have that $[\overrightarrow{w}\ a\ \overleftarrow{w}] \in M_g$.

$\square$

## 2.2 Folded Polynomials

We define the set of all *folded polynomials* in $\mathbb{F}_q[x]$ recursively as follows.

1. If $r$ is a monic polynomial of degree 1 then $r$ is folded.

2. If $r$ is folded then $r^2$ and $ar^2$ are folded, where $a$ is a monic polynomial of degree 1.

The motivation for this definition comes from [10] in which a class of continued fractions dubbed 'folded continued fractions' is studied by van der Poorten and Shallit; the denominators of certain types of 'folded continued fractions' are folded polynomials, as we define them.

It is easily seen that folded polynomials are monic and split into linear factors. In fact, it is a simple matter to classify which polynomials of this form are folded. (We write $n = (\alpha_0\alpha_1\alpha_2\ldots)_2$ to indicate that $n = \sum_{i\geq 0}\alpha_i 2^i$ where $\alpha_i = 0$ or $1$ for $i \geq 0$.)

**Proposition 3** *Let $g \in \mathbb{F}_q[x]$, $char\,\mathbb{F}_q = 2$, with $g = a_1^{m_1}a_2^{m_2}\ldots a_k^{m_k}$ where $a_j$ is monic of degree 1 and $m_j = (\alpha_0^j\alpha_1^j\alpha_2^j\ldots)_2$ for $1 \leq j \leq k$. Then $g$ is folded if and only if $\alpha_i^{j_1}\alpha_i^{j_2} = 0$ for all $1 \leq j_1 \neq j_2 \leq k$ and $i \geq 0$.*

*Proof:* For the sake of clarity we only consider the case $q = 2$; the general case is proved in an analogous fashion.

Let $g$ be a folded polynomial over $\mathbb{F}_2$. Then $g$ splits into linear factors and we may write $g = x^{m_1}(x+1)^{m_2}$ where $m_1 = (\alpha_0\alpha_1\alpha_2\ldots)_2$ and $m_2 = (\beta_0\beta_1\beta_2\ldots)_2$. If $deg\,g = 1$ then $\alpha_i\beta_i = 0$ for $i \geq 0$. Let $deg\,g > 1$. Observe that since $g$ is folded at most one of $m_1$ and $m_2$ can be odd. Firstly, suppose that $m_1$ and $m_2$ are even, so $\alpha_0 = \beta_0 = 0$. Then $g = h^2$ where $h = x^{l_1}(x+1)^{l_2}$ is a folded polynomial with $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. We may assume by induction that $\alpha_i\beta_i = 0$ for $i \geq 1$. Hence $\alpha_i\beta_i = 0$ for $i \geq 0$. Suppose now that $m_1$ is odd and $m_2$ is even, so $\alpha_0 = 1$ and $\beta_0 = 0$. Then $g = xh^2$ where $h = x^{l_1}(x+1)^{l_2}$ is a folded polynomial with $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. Once again, we may assume by induction that $\alpha_i\beta_i = 0$ for $i \geq 1$. So $\alpha_i\beta_i = 0$ for $i \geq 0$, as required. The remaining case, $m_0$ even and $m_1$ odd, follows in the same way.

Conversely, let $\alpha_i\beta_i = 0$ for $i \geq 0$. If $deg\,g = 1$ then $g$ is folded. Let $deg\,g > 1$. We have that $\alpha_0\beta_0 = 0$ and so there are three possibilities for the pair $\alpha_0, \beta_0$: either $\alpha_0 = \beta_0 = 0$; $\alpha_0 = 1$ and $\beta_0 = 0$; or $\alpha_0 = 0$ and $\beta_0 = 1$.

If $\alpha_0 = \beta_0 = 0$ then $g = h^2$ for some polynomial $h$. Now $h = x^{l_1}(x+1)^{l_2}$ where $l_1 = (\alpha_1\alpha_2\ldots)_2$ and $l_2 = (\beta_1\beta_2\ldots)_2$. Since $\alpha_i\beta_i = 0$ for $i \geq 1$ we may assume by induction that $h$ is folded. Hence $g$ is folded. The remaining two cases are proved in a similar way.

$\square$

## 3 Theorems

Our main theorem reveals the intimate connection between polynomials with certain orthogonal multiplicities and the folded polynomials we have described.

**Theorem 4** *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and let $g$ be a monic polynomial over $\mathbb{F}_q$. Then $g$ has odd orthogonal multiplicity if and only if $g$ is folded.*

*Proof:* Let $g$ be a monic polynomial. We first prove that if $g$ has odd multiplicity then $g$ is folded. To be more precise, we show that if $g$ has odd multiplicity and $deg\, g > 1$ then $g = ah^2$ where $a = 1$ or $a$ is monic of degree 1, and where $h$ is monic and has odd multiplicity. The result then follows by induction from the fact that all monic polynomials of degree 1 are folded.

Let $g$ have odd multiplicity with $deg\, g > 1$. Let $\theta$ denote the map that acts on the set $\{r/s \in \mathbb{F}_q(x) \mid deg\, r < deg\, s\}$ and sends the continued fraction $[\overrightarrow{w}]$ to the continued fraction $[\overleftarrow{w}]$. Then the set $M_g$ is invariant under $\theta$ by Lemma 2 Part 1, and $\theta$ is an involution. Since $|M_g|$ is odd, there must exist an element of $M_g$ which is fixed by $\theta$. The involution $\theta$ fixes a continued fraction if and only if it is symmetric. So there exists a symmetric continued fraction $[\,v\,]$ in $M_g$. There are two cases to consider.

Firstly, suppose that $deg\, g$ is odd. Then by the observation preceding Lemma 2, $v = \overrightarrow{w}\ a\ \overleftarrow{w}$ for some word $w$ and polynomial $a$ of degree 1, and we have that $[\,\overrightarrow{w}\ a\ \overleftarrow{w}\,] \in M_g$. Let $a = kb$ where $k \in \mathbb{F}_q^*$ and $b$ is monic. Then by Lemma 2 Part 3(i), $g = bh^2$ where $h$ is monic and $[\,\overrightarrow{w}\,] \in M_h$. We need to show that $h$ has odd multiplicity. Suppose then that $m(h)$ is even. Let $U = \{[\,\overrightarrow{w}\ c\ \overleftarrow{w}\,] \,|\, [\,\overrightarrow{w}\,] \in M_h,\, c = lb,\, l \in \mathbb{F}_q^*\}$. Since every continued fraction in $U$ is symmetric, $U$ is invariant under the involution $\theta$, and by Lemma 2 Part 3(ii), we have that $U \subseteq M_g$. Hence $M_g - U$ is invariant under $\theta$. Now $|U| = (q-1)|M_h| = (q-1)m(h)$, an even number. Therefore $|M_g - U|$ is odd, and so there must be a symmetric continued fraction $[\,\overrightarrow{u}\ d\ \overleftarrow{u}\,]$ in $M_g - U$ where $u$ is a word and $d$ is a polynomial of degree 1. Now $[\,\overrightarrow{u}\,] \in M_r$ for some unique monic $r$, and $d = le$ where $e$ is monic and $l \in \mathbb{F}_q^*$. By Lemma 2 Part 3(i), $g = er^2$, and so $er^2 = bh^2$. If $e \neq b$ then $e$ would occur as a factor an odd number of times on the left-hand side of this equation and an even number of times on the right-hand side. Therefore $e = b$ and so $r = h$, since $char\, \mathbb{F}_q = 2$. But then $[\,\overrightarrow{u}\,] \in M_h$, and so $[\,\overrightarrow{u}\ d\ \overleftarrow{u}\,] \in U$. This is a contradiction and so $m(h)$ must be odd.

Suppose now that $deg\, g$ is even. Then by our previous observation, $v = \overrightarrow{w}\,\overleftarrow{w}$ for some word $w$, and so $[\,\overrightarrow{w}\,\overleftarrow{w}\,] \in M_g$. Let $h$ be the unique monic polynomial such that $[\,\overrightarrow{\phi(w)}\,] \in M_h$. Then by Lemma 2 Part 2(i), we have that $g = h^2$. We argue by contradiction to prove that $m(h)$ is odd. Suppose $m(h)$ is even. Let $U = \{[\,\overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}\,] \,|\, [\,\overrightarrow{w}\,] \in M_h\}$. Then by Lemma 2 Part

2(ii), $U \subseteq M_g$ and we further have that $M_g - U$ is invariant under the involution $\theta$. Now $|U| = |M_h|$ is even and so $|M_g - U|$ is odd, and there must be a symmetric continued fraction, $[\,\overrightarrow{u}\,\overleftarrow{u}\,]$ say, in $M_g - U$. Letting $r$ be the unique monic polynomial such that $[\,\overrightarrow{\phi(u)}\,] \in M_r$, we find by Lemma 2 Part 2(ii) that $r^2 = g = h^2$, and so $r = h$, as $char\, \mathbb{F}_q = 2$. Hence $[\,\overrightarrow{\phi(u)}\,] \in M_h$ and so, since $\phi$ is an involution, $[\,\overrightarrow{u}\,\overleftarrow{u}\,] \in U$, which is a contradiction. Therefore $m(h)$ is odd.

We now show by induction on $deg\, g$ that if $g$ is a folded polynomial then the multiplicity of $g$ is odd. Let $g$ be a folded polynomial. If $deg\, g = 1$ then $K(k/g) = 1$ for all $k \in \mathbb{F}_q^*$ and so $g$ has multiplicity $q - 1$. Let $deg\, g > 1$. We must consider two cases.

Firstly, suppose $deg\, g$ is odd. Then $g = bh^2$ where $h$ is folded and $b$ is monic of degree 1. We may assume by induction that $m(h)$ is odd. We argue by contradiction to prove that $m(g)$ is odd. Suppose that $m(g)$ is even. Let $U = \{[\,\overrightarrow{w}\; c\; \overleftarrow{w}\,] \,|\, [\,\overrightarrow{w}\,] \in M_h,\, c = lb, l \in \mathbb{F}_q^*\}$. Then $U \subseteq M_g$ by Lemma 2 Part 3(ii), and $M_g - U$ is invariant under the involution $\theta$. Now $|U| = (q-1)|M_h| = (q-1)m(h)$, an odd number, and so $|M_g - U|$ is also odd. Therefore $M_g - U$ contains a symmetric continued fraction $[\,\overrightarrow{u}\; d\; \overleftarrow{u}\,]$ where $u$ is a word and $d$ is a polynomial of degree 1. If we let $r$ be the unique monic polynomial such that $[\,\overrightarrow{u}\,] \in M_r$, and let $d = le$ where $e$ is monic and $l \in \mathbb{F}_q^*$, we have that $er^2 = bh^2$. As before, we conclude that $r = h$ and so $[\,\overrightarrow{u}\; d\; \overleftarrow{u}\,] \in U$, which is a contradiction. Therefore $m(g)$ is odd.

Suppose now that $deg\, g$ is even. Then $g = h^2$ where $h$ is folded. We may assume by induction that $m(h)$ is odd. Suppose that $m(g)$ is even.

Let $U = \{[\,\overrightarrow{\phi(w)}\,\overleftarrow{\phi(w)}\,] \,|\, [\,\vec{w}\,] \in M_h\}$. Once again, $U \subseteq M_g$ by Lemma 2 Part 2(ii), and $|U| = |M_h|$ is odd. So $|M_g - U|$ is odd and $M_g - U$ must contain a symmetric continued fraction $[\,\vec{u}\,\overleftarrow{u}\,]$. If we let $r$ be the unique monic polynomial such that $[\,\overrightarrow{\phi(u)}\,] \in M_r$, then $r^2 = g = h^2$ and so $r = h$. We then have that $[\,\vec{u}\,\overleftarrow{u}\,] \in U$, which is a contradiction. So $m(g)$ is odd. This completes the proof.

□

It is observed by Niederreiter in [7] that the expected value for the orthogonal multiplicity of a polynomial of degree $n$ over $\mathbb{F}_q$ is $(q-1)^n$, and it is easily shown that the orthogonal multiplicity of such a polynomial is no greater than $(q-1)^{\lceil n/2 \rceil} q^{\lfloor n/2 \rfloor}$. There are, however, no known non-trivial lower bounds on the multiplicity of an arbitrary polynomial. Theorem 5 gives us a lower bound on the multiplicity of a folded polynomial.

**Theorem 5** *Let $g \in \mathbb{F}_q[x]$, $char\, \mathbb{F}_q = 2$, be a folded polynomial of degree $n$. Let $wt(n)_2$ denote the weight of the binary representation of $n$. Then $m(g) \geq (q-1)^{wt(n)_2}$.*

*Proof:* We prove by induction on $deg\, g$ that if $g$ is folded then $m(g) \geq (q-1)^{wt(n)_2}$, where $n = deg\, g$ and $wt(n)_2$ denotes the weight of the binary representation of $n$. Let $g \in \mathbb{F}_q[x]$, $char\, \mathbb{F}_q = 2$, be a folded polynomial. If $deg\, g = 1$ then $K(k/g) = 1$ for all $k \in \mathbb{F}_q^*$ and so $m(g) = (q-1) = (q-1)^{wt(1)_2}$. So let $deg\, g > 1$.

Suppose that $deg\, g = n$ is even. Then $g = h^2$ where $h$ is folded of degree $n/2$. We may assume by induction that $m(h) \geq (q-1)^{wt(n/2)_2}$.

From the proof of the even case of the second part of Theorem 4, it is clear that $m(g) \geq m(h)$. Now $wt(n)_2 = wt(n/2)_2$ and so we have that $m(g) \geq m(h) \geq (q-1)^{wt(n/2)_2} = (q-1)^{wt(n)_2}$.

Suppose now that $deg\, g = n$ is odd. Then $g = bh^2$ where $h$ is folded of degree $(n-1)/2$ and $b$ is a monic polynomial of degree 1. We may assume by induction that $m(h) \geq (q-1)^{wt((n-1)/2)_2} = (q-1)^{wt(n)_2-1}$. Define the set $U$ as in the odd case of the second part of Theorem 4. Then $m(g) = |M_g| \geq |U| = (q-1)|M_h| = (q-1)m(h)$. Since $m(h) \geq (q-1)^{wt(n)_2-1}$ we have $m(g) \geq (q-1)m(h) \geq (q-1)^{wt(n)_2}$ as required.

$\square$

# 4 Further Results

As we have mentioned before, the orthogonal multiplicity of a polynomial over a finite field $\mathbb{F}_q$ is a multiple of $q-1$ and so a polynomial over $\mathbb{F}_q$ with positive multiplicity must have multiplicity at least $q-1$. If a polynomial $g$ over $\mathbb{F}_q$ has multiplicity exactly $q-1$ then this means that there exists a unique monic $f$, of degree less than that of $g$ and coprime to $g$, such that $K(f/g) = 1$. Theorem 5 has as a corollary a classification of all polynomials with multiplicity $q-1$ over finite fields of even order $q \neq 2$.

**Corollary 6** *Let $g$ be a monic polynomial in $\mathbb{F}_q[x]$, $char\, \mathbb{F}_q = 2$, with $q \neq 2$. Then $m(g) = q-1$ if and only if $g$ has degree 1.*

*Proof:* If $g$ is a monic polynomial of degree 1 then $K(k/g) = 1$ for all $k \in \mathbb{F}_q^*$ and so $m(g) = q-1$. Conversely, let $g \in \mathbb{F}_q[x]$, $char\, \mathbb{F}_q = 2$, have multiplicity $q-1$. By Theorem 4, $g$ is a folded polynomial. If $deg\, g = n$ then we must have by Theorem 5 that $wt(n)_2 = 1$, that is to say, $n = 2^m$ for some $m$. We claim that the only folded polynomials of degree $2^m$ for some $m \geq 0$ are those of the form $a^{2^m}$, where $a$ is a monic polynomial of degree 1. This is easily proved by observing that if $s$ is folded of degree $2^m$ then $s = t^2$ for some folded polynomial of degree $2^{m-1}$. We may assume by induction that $t = a^{2^{m-1}}$ for some monic polynomial $a$ of degree 1. Thus $s = a^{2^m}$. Therefore we must have that $g = a^{2^m}$ for some monic polynomial $a$ of degree 1. We now prove by induction on $m \geq 1$ that $m(a^{2^m}) \geq m(a^2)$. Certainly $m(a^{2^1}) \geq m(a^2)$. Assume now that $m(a^{2^{m-1}}) \geq m(a^2)$ for some $m \geq 2$. It is clear from the proof of the even case of the second part of Theorem 4 that $m(a^{2^m}) = m((a^{2^{m-1}})^2) \geq m(a^{2^{m-1}})$. So $m(a^{2^m}) \geq m(a^2)$ as required. Finally, observe that if $deg\, b = 1$ and $b \neq la$, $l \in \mathbb{F}_q^*$, then $\gcd(b, a^2) = 1$ and $K(b/a^2) = 1$. So $m(a^2) = (q-1)^2 > q-1$, since $q \neq 2$. Hence $m(a^{2^m}) > q-1$ for $m \geq 1$. We must therefore have that $g = a$ where $a$ is a monic polynomial of degree 1.

□

In [1] Blackburn shows that a polynomial $g$ over $\mathbb{F}_2$ has orthogonal multiplicity 1 if and only if it is of the form $x^{m_1}(x+1)^{m_2}$ where $\binom{m_1+m_2}{m_2} \equiv 1 \bmod 2$. It is of interest that Theorem 4 can also be used to obtain an alternative, but of course equivalent, classification of polynomials of multiplicity 1 over $\mathbb{F}_2$. (This equivalence can be seen directly from the Lucas congruence for binomial coefficients [5].)

**Corollary 7** *Let $g \in \mathbb{F}_2[x]$. Then $g$ has orthogonal multiplicity 1 if and* *only if* $g = x^{m_1}(x+1)^{m_2}$ *where* $m_1 = (\alpha_0\alpha_1\alpha_2\ldots)_2$, $m_2 = (\beta_0\beta_1\beta_2\ldots)_2$ *and* $\alpha_i\beta_i = 0$ *for* $i \geq 0$.

*Proof:* Let $g \in \mathbb{F}_2[x]$. We claim that $g$ has multiplicity 1 if and only if $g$ is folded. By Theorem 4, if $g$ has multiplicity 1 then $g$ is folded. Conversely, if $g$ is folded then it must have odd multiplicity. Blackburn proves in [1] that if a polynomial $g$ over $\mathbb{F}_2$ has positive multiplicity then it must have multiplicity $2^k$, where $k$ is the number of distinct non-linear irreducible factors of $g$. Therefore a polynomial over $\mathbb{F}_2$ which has odd multiplicity must have multiplicity 1. This proves the claim. The result now follows from the characterization of folded polynomials given in Proposition 3.

□

By the result from [1] mentioned in the proof of the above corollary, if a polynomial over $\mathbb{F}_2$ which splits into linear factors has positive orthogonal multiplicity then it must have multiplicity $2^0 = 1$. Therefore by the above corollary, there exist polynomials over $\mathbb{F}_2$ which split into linear factors which have multiplicity zero. We show, however, that if $g$ is a polynomial over $\mathbb{F}_2$ which splits into linear factors then there exists a polynomial $f$ over $\mathbb{F}_2$ with $\gcd(f,g) = 1$ such that $K(f/g) \leq 2$. This proves a special case of the following conjecture made by Mesirov and Sweet in [6]: if $g \in \mathbb{F}_2[x]$ then there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f,g) = 1$ such that $K(f/g) \leq 2$.

**Proposition 8** *If* $g \in \mathbb{F}_2[x]$ *splits into linear factors then there exists* $f \in \mathbb{F}_2[x]$ *with* $\gcd(f,g) = 1$ *such that* $K(f/g) \leq 2$.

*Proof:* Let $g \in \mathbb{F}_2[x]$ with $g = x^{m_1}(x+1)^{m_2}$. We prove by induction on *deg* $g$ that there exists $f \in \mathbb{F}_2[x]$ with $\gcd(f, g) = 1$ such that $K(f/g) \leq 2$.

If *deg* $g = 1$ then we have that $K(1/g) = 1$. Let *deg* $g > 1$. If $m_1$ and $m_2$ are even then we may write $g = s^2$ where $s$ splits into linear factors. We may assume by induction that there exists $r \in \mathbb{F}_2[x]$ with $\gcd(r, s) = 1$ and $K(r/s) \leq 2$. Without loss of generality, we may further assume that *deg* $r <$ deg $s$, and so $r/s = [\, w\, ]$ for some $w = a_1 a_2 \ldots a_m$ with *deg* $a_i \leq 2\,(1 \leq i \leq m)$. Let $r_m/s_m$ denote the $m^{th}$ convergent of $[\, w\, ]$. Then $r_m/s_m = [\, w\, ] = r/s$ and $\gcd(r_m, s_m) = 1$. Hence, since we are working over $\mathbb{F}_2$, $r = r_m$ and $s = s_m$. By Lemma 1 Part 2, $(rs+1)/g = (rs+1)/s^2 = [\, \overrightarrow{\phi(w)}\ \overleftarrow{\phi(w)}\, ]$, and we also have that $\gcd(rs+1, g) = \gcd(rs+1, s^2) = 1$. Finally, since *deg* $a_i \leq 2$ for $1 \leq i \leq m$, we have that $K((rs+1)/g) \leq 2$.

If at least one of $m_1$ and $m_2$ is odd then we may write $g = as^2$ where $1 \leq$ *deg* $a \leq 2$ and $s$ splits into linear factors. We may assume by induction that there exists $r \in \mathbb{F}_2[x]$ with $\gcd(r, s) = 1$ and $K(r/s) \leq 2$. We may further assume that *deg* $r <$ *deg* $s$, and so $r/s = [\, w\, ]$ for some $w = a_1 a_2 \ldots a_m$ with *deg* $a_i \leq 2\,(1 \leq i \leq m)$. Let $r_m/s_m$ denote the $m^{th}$ convergent of $r/s$. We have that $r = r_m$ and $s = s_m$, and so by Lemma 1 Part 3, $(ars+1)/g = (ars+1)/as^2 = [\, \overrightarrow{w}\ a\ \overleftarrow{w}\, ]$. Certainly, $\gcd(ars+1, g) = \gcd(ars+1, as^2) = 1$. By assumption *deg* $a_i \leq 2$ for $1 \leq i \leq m$, and we further have that *deg* $a \leq 2$. Hence $K((ars+1)/g) \leq 2$, which completes the proof.

$\square$

## 5 Comments

One may define folded polynomials over finite fields $\mathbb{F}_q$ of odd characteristic in an obvious way; however, few of the results which hold for folded polynomials in characteristic 2 are still true. A plausible analogue of Theorem 4, that a polynomial has orthogonal multiplicity $k(q-1)$ where $k$ is odd if and only if it is folded, is, in general, false. For example, over $\mathbb{F}_3$ the folded polynomial $x^3$ has multiplicity 8, and the polynomial $x^3 + x = x(x^2+1)$ has multiplicity 6. One may show, however, that if $g$ is a folded polynomial over $\mathbb{F}_q$ with $deg\, g = n$ then $m(g) \geq (q-1)^{wt(n)_2}$, and, of course, an odd characteristic analogue of Proposition 3 is still true. It also seems reasonable to conjecture that over a finite field $\mathbb{F}_q$ of odd characteristic a polynomial has multiplicity $q-1$ if and only if it is linear.

Niederreiter asks the following question in [9]: does there exist a constant $C_q$ such that if $g \in \mathbb{F}_q[x]$ then there exists $f \in \mathbb{F}_q[x]$ with $\gcd(f,g) = 1$ such that $K(f/g) \leq C_q$? As we have mentioned before, Blackburn [1] conjectures that $C_q = 1$ for $q \neq 2$ and Mesirov and Sweet [6] believe that $C_2 = 2$. It is of some interest that this question is essentially a rational function analogue of a long-standing conjecture in number theory known as 'Zaremba's conjecture' [12]: for any integer $n$ there exists an integer $m$ coprime to $n$ such that all the partial quotients of the (simple) continued fraction expansion of $m/n$ are no greater than 5.

## References


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

[2] S.R. Blackburn, Linear cellular automata as stream cipher components, preprint, University of London, (1997).

[3] K. Cattell and J.C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, *IEEE Trans. Comp. Aided Design of Integrated Systems* **15** No.3, (1996), 325-335.

[4] R. Lidl and H. Niederreiter, "Finite Fields", 2nd Edition, Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[5] E. Lucas, Sur les congruences des nombres Euleriennes, et des coefficients différentials des functions trigonométriques, suivant un-module premier, *Bull. Soc. Math. France* **6**, (1878), 49-54.

[6] J.P. Mesirov and M.M. Sweet, Continued fraction expansion of rational expressions with irreducible denominators in characteristic 2, *J. Number Theory* **27**, (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: Proc. Eurocrypt 87", D. Chaum and W.L. Price (Eds), Springer, Berlin, 37-51, 1988.

[9] H. Niederreiter, Continued fraction expansions of rational functions, in "Finite Fields, Coding Theory, and Advances in Comm. and Computing", G.L. Mullen and P.J.-S. Shuie (Eds), Lect. Notes in Pure and Appl. Math., Vol. 141. Marcel Dekker, New York, 433-434, 1993.

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

[11] G. Szegő, "Orthogonal Polynomials", American Math. Soc., New York, 1959.

[12] S.K. Zaremba, La méthode des "bons treillis" pour le calcul des intégrales multiples, in "Applications of Number Theory to Numerical Analysis", S.K. Zaremba (Ed), Academic Press, New York, 39-119, 1972.