Explicit Sequence Expansions

David Kohel, San Ling, and Chaoping Xing

Department of Mathematics
National University of Singapore
Kent Ridge Crescent, Singapore 119260
Email: kohel,matlings,xingcp@math.nus.edu.sg

Abstract. Examples of d-perfect sequences are constructed based on the method in Xing *et al* [8]. In particular examples of 1-perfect sequences based on genus 0 curves over binary and the ternary fields are computed, as are 2-perfect binary sequences based on an elliptic curve. The complexity profile of certain of the 2-perfect sequences are experimentally determined to follow that of 1-perfect sequences. Based on two algebraic reformulations of the known characterization of binary 1-perfect sequences, these sequences are proved to be 1-perfect.

1 Introduction

In the previous articles [8] and [9] of Xing *et al.*, several constructions of d-perfect sequences are given based on functions on a curve over a finite field. The freedom to choose a local parameter and a function on a curve (see Theorem 1) allows many different d-perfect sequences to be derived from a given curve. In this paper, we present a method to compute these d-perfect sequences, and give examples of d-perfect sequences, for small d, by choosing functions of small degree on a curve.

The choice of the curve as well as the functions permits great flexibility in constructing d-perfect sequences. With the interest of considering curves which admit functions of small degree, we will concentrate on curves of genera 0 and 1, namely, the projective line and elliptic curves. This paper is arranged in the following way. In Section 2, some notations concerning d-perfect sequences and a result regarding the construction of d-perfect sequences in Xing *et al.* [8] will be recalled. Those 1-perfect sequences given by this construction using the curves of genus 0 over the binary and ternary fields are completely listed in Section 3. Section 4 is devoted to an example of sequences derived from an elliptic curve over $\mathbf{F}_2$. Certain 2-perfect sequences constructed in this manner are experimentally observed to be 1-perfect to a high degree of accuracy. This observation is proved based on two algebraic reformulations of the known characterization of binary 1-perfect sequences. The reformulations themselves give infinite families of binary 1-perfect sequences constructed as series expansion of functions on curves and on surfaces.

2 Background

Let us first recall some concepts regarding d-perfect sequences over a finite field $\mathbf{F}_q$ of q elements. For a sequence $\mathbf{s}$ of finite length, we denote by $\ell_{\mathbf{s}}$ the linear complexity of $\mathbf{s}$. Thus we obtain the linear complexity profile (simply denoted by *lcp*) for an infinite sequence $\mathbf{a}$, namely, the integer sequence

$$\{\ell_{\mathbf{a}}(n)\}_{n=1}^{\infty},$$

where $\ell_{\mathbf{a}}(n)$ is the linear complexity of the first n terms of the sequence $\mathbf{a}$. The sequence $\mathbf{a}$ is called d-perfect for a positive integer d if the following condition holds:

$$\frac{n+1-d}{2} \leq \ell_{\mathbf{a}}(n) \leq \frac{n+d}{2} \quad \text{for all } n.$$

Definition. Let $\mathcal{X}/\mathbf{F}_q$ be a curve and x a function in $\mathbf{F}_q(\mathcal{X})$. The *degree* of a nonconstant x is defined to be the degree of the field extension $\mathbf{F}_q(\mathcal{X})/\mathbf{F}_q(x)$, and a constant function x is defined to have degree zero.

For a function x of $\mathbf{F}_q(\mathcal{X}) - \{0\}$, let $\mathrm{div}(x)$ be the principal divisor associated with x. Put

$$\mathrm{div}(x) = \mathrm{div}_0(x) - \mathrm{div}_\infty(x),$$

where $\mathrm{div}_0(x)$ and $\mathrm{div}_\infty(x)$ are two effective divisors and the supports of $\mathrm{div}_0(x)$ and $\mathrm{div}_\infty(x)$ are disjoint. Then $\mathrm{div}_0(x)$ and $\mathrm{div}_\infty(x)$ are uniquely determined by x and $\deg(\mathrm{div}_0(x))$ is equal to the degree of x. Let v_P denote the normalized discrete valuation corresponding to the point P on $\mathcal{X}/\mathbf{F}_q$.

We apply the following theorem to the explicit construction of d-perfect sequences (see Theorem 3.1 of [8]).

Theorem 1. *Let $\mathcal{X}/\mathbf{F}_q$ be a curve for which there exist an $\mathbf{F}_q$-rational point P on $\mathcal{X}$ and a degree 2 function t in $\mathbf{F}_q(\mathcal{X})$ such that $v_P(t) = 1$. Let x be a function of degree d on $\mathcal{X}$ such that $\mathbf{F}_q(\mathcal{X}) = \mathbf{F}_q(x,t)$ with $(x/t)(P) = 1$. Then there exists a unique power series expansion of the form*

$$x(t) = t + a_2 t^2 + a_3 t^3 + a_4 t^4 + \cdots$$

for x which defines an embedding of the function field $\mathbf{F}_q(\mathcal{X})$ in $\mathbf{F}_q((t))$. The corresponding sequence $(1, a_2, a_3, a_4, \dots)$ is d-perfect.

If the sequence of coefficients of a series $x(t)$ is d-perfect we say that the series is d-perfect. The series $x(t)$ can be rapidly computed via the effective form of Hensel's lemma (see Chapter II, Proposition 2 of Lang [1]).

Theorem 2 (Hensel's Lemma). *Let x and t be as in the previous theorem, and let x have minimal polynomial $F(X)$ over $\mathbf{F}_q(t)$. Then the power series expansion for x in $\mathbf{F}_q((t))$ can be determined by setting $x_1(t) = t$, and for all i,*

$$x_{i+1} = x_i - \frac{F(x_i)}{F'(x_i)},$$

where $F'(X)$ is the derivative of $F(X)$ with respect to X, and the sequence (x_i) satisfies $v_P(F(x_i)) \geq 2^i$.

3 Genus zero curves

3.1 General theory

To obtain 1-perfect sequences using the above construction, we require a curve $\mathcal{X}/\mathbf{F}_q$ which has a degree one function x. Such a curve has function field $\mathbf{F}_q(x)$ and it is immediately seen that it is of genus zero. Thus we begin with a pair of a genus zero curve $\mathcal{X}/\mathbf{F}_q$ and a function x generating $\mathbf{F}_q(\mathcal{X})$. Let P be the zero of x, and let t be a degree two function on $\mathcal{X}$ such that $v_P(t) = 1$ and $(x/t)(P) = 1$. The form of t is described by means of the following proposition.

Proposition 1. *Let $\mathcal{X}/\mathbf{F}_q$ be a genus zero curve with $\mathbf{F}_q(\mathcal{X}) = \mathbf{F}_q(x)$, and let P be the zero of x. A degree two function $t \in \mathbf{F}_q(x)$ satisfying $(x/t)(P) = 1$ has the form*

$$t = \frac{x + ax^2}{1 + bx + cx^2}$$

for some a, b, and c in $\mathbf{F}_q$, and where a or c is nonzero, and $\gcd(1 + ax, 1 + bx + cx^2) = 1$.

Every generator x_1 for the rational function field $\mathbf{F}_q(x)$ is of the form

$$x_1 = \frac{ax + b}{cx + d},$$

where a, b, c, and d are elements of the base field $\mathbf{F}_q$ with $ad - bc \neq 0$. Given any x_1 in $\mathbf{F}_q(x)$ and a point P on $\mathcal{X}$, we may replace it with $x_1 - x_1(P)$. Thus by scaling we may assume that

$$v_P(x_1) = 1, \quad \text{and} \quad (x_1/x)(P) = 1.$$

Then $x_1(P) = b/d = 0$, and $(x_1/x)(P) = a/d = 1$. Thus any degree one function x_1 can be normalized such that it is of the form

$$x_1 = \frac{x}{1 + cx}.$$

By Theorem 1, the corresponding power series expansion for x_1 in t is also 1-perfect, which proves the following proposition.

Proposition 2. *Suppose x_0 and x_1 are degree one functions on a curve $\mathcal{X}$ and t is a degree two uniformizing parameter at a point P. Suppose moreover that $v_P(x_0) = v_P(x_1) = 1$ and $(x_1/x_0)(P) = 1$. Then x_1 is of the form*

$$x_1 = \frac{x_0}{1 + cx_0},$$

and the series $x_0(t)$ and $x_1(t)$ are both 1-perfect.

3.2 1-Perfect sequences over $\mathbf{F}_2$

From Proposition 1, we see that there are four possible choices for the degree two local parameter t over the binary field. These are:

$$(0.0)\ t = x + x^2, \qquad (1.0)\ t = \frac{x + x^2}{1 + x + x^2},$$

$$(0.1)\ t = \frac{x}{1 + x^2}, \qquad (1.1)\ t = \frac{x}{1 + x + x^2}.$$

In this case Hensel's lemma construction for a power series solution $x = x(t)$ to one of the above equations is a special case of a reversion formula for power series. That is, if we take equation $(i.j)$ to define the power series $t(x)$ in $\mathbf{F}_2[x]$, then $t(x(t)) = t$ and $x(t(x)) = x$.

We note that the linear fractional transformation $A(u) = u/(1 + u)$ determines an automorphism of order two of the projective line $\mathbf{P}^1(\mathbf{F}_2)$. If we denote by $x_{ij}(t)$ the power series which is a root of equation $(i.j)$, and set $x(t) = x_{00}(t)$, then

$$x_{ij}(t) = A^j(x(A^i(t))).$$

We find the following sequences associated to the t-expansions of x in the four cases.

(0.0) $(1,1,0,1,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\ldots)$,
(0.1) $(1,0,1,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,\ldots)$,
(1.0) $(1,0,1,1,1,0,1,0,1,0,1,1,1,0,1,1,1,0,1,1,1,0,1,0,1,0,1,1,1,0,1,\ldots)$,
(1.1) $(1,1,0,0,1,1,1,1,1,1,0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,1,0,0,1,1,1,\ldots)$.

These initial segments can be verified to follow the linear complexity of 1-perfect sequences.

The sequence (0.0) is the well-known 1-perfect sequence of the power series (see [2–5, 7]).

$$\sum_{i=0}^{\infty} t^{2^i} = t + t^2 + t^4 + t^8 + t^{16} + \cdots,$$

and the sequence (0.1) is that of the power series

$$\sum_{i=1}^{\infty} t^{2^i - 1} = t + t^3 + t^7 + t^{15} + t^{31} + \cdots,$$

By making the substitution $t \mapsto t/(1+t)$, the corresponding sequences (1.0) and (1.1) can be seen to have the forms

$$\sum_{m=1}^{\infty} \sum_{i=0}^{\infty} t^{m2^i} \quad \text{and} \quad \sum_{m=1}^{\infty} \sum_{i=0}^{\infty} t^{m(2^i-1)},$$

respectively.

3.3 1-Perfect sequences over $\mathbf{F}_3$

From Proposition 1 we see that there are 18 possible choices of degree 2 local parameters t over $\mathbf{F}_3$, which we subdivide into a block of nine functions:

$$(0.0)\ t = \frac{x}{1+x+x^2}, \quad (1.0)\ t = \frac{x}{1-x+x^2}, \quad (2.0)\ t = \frac{x}{1+x^2},$$

$$(0.1)\ t = x + x^2, \quad (1.1)\ t = \frac{x+x^2}{1+x+x^2}, \quad (2.1)\ t = \frac{x+x^2}{1-x-x^2},$$

$$(0.2)\ t = \frac{x-x^2}{1-x+x^2}, \quad (1.2)\ t = x - x^2, \quad (2.2)\ t = \frac{x-x^2}{1+x-x^2}.$$

and a second block of nine functions:

$$(0.0)\ t = \frac{x}{1-x^2}, \quad (1.0)\ t = \frac{x}{1+x-x^2}, \quad (2.0)\ t = \frac{x}{1-x-x^2},$$

$$(0.1)\ t = \frac{x+x^2}{1-x}, \quad (1.1)\ t = \frac{x+x^2}{1+x^2}, \quad (2.1)\ t = \frac{x+x^2}{1+x-x^2},$$

$$(0.2)\ t = \frac{x-x^2}{1+x}, \quad (1.2)\ t = \frac{x-x^2}{1-x-x^2}, \quad (2.2)\ t = \frac{x-x^2}{1+x^2}.$$

The linear fractional transformation $A(u) = u/(1+u)$ determines an automorphism of $\mathbf{P}^1(\mathbf{F}_3)$ of order three. As in Section 3.2, it is easy to verify that roots of any two equations in the same block can be exchanged by action of the group $\langle A \rangle$. Since A generates the group of automorphisms of $\mathbf{P}^1(\mathbf{F}_3)$ which fix the point $P = (0:1)$ and the residue of functions at P, we may think of each of the two blocks of equations as comprising an equivalence class over $\mathbf{F}_3$. The corresponding sequences for the first block are:

(0.0) $(1,1,2,1,0,0,0,1,2,1,1,2,1,0,0,0,0,0,0,0,0,0,0,0,0,1,2,1,1,2,1,\ldots)$,
(0.1) $(1,2,2,1,2,0,0,0,2,1,2,2,1,2,0,0,0,0,0,0,0,0,0,0,0,2,1,2,2,1,\ldots)$,
(0.2) $(1,0,1,1,0,0,0,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,\ldots)$,

(1.0) $(1,2,2,2,0,0,0,2,2,2,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,2,2,2,1,1,1,\ldots)$,
(1.1) $(1,0,1,2,0,0,0,0,1,2,0,2,1,0,0,0,0,0,0,0,0,0,0,0,0,1,2,0,2,1,\ldots)$,
(1.2) $(1,1,2,2,2,0,0,0,2,2,2,1,1,1,0,0,0,0,0,0,0,0,0,0,0,2,2,2,1,1,\ldots)$,

(2.0) $(1,0,1,0,2,0,2,0,2,0,0,0,0,0,0,0,2,0,2,0,2,0,1,0,1,0,1,0,0,0,0,\ldots)$,
(2.1) $(1,1,2,0,0,1,2,2,1,0,0,0,0,0,0,0,0,1,2,2,1,0,0,2,1,1,2,0,0,0,0,\ldots)$,
(2.2) $(1,2,2,0,0,2,2,1,1,0,0,0,0,0,0,0,0,2,2,1,1,0,0,1,1,2,2,0,0,0,0,\ldots)$,

and for the second block:

(0.0) $(1,0,2,0,2,0,1,0,2,0,0,0,0,0,0,0,2,0,1,0,2,0,2,0,1,0,2,0,0,0,0,\ldots)$,
(0.1) $(1,1,0,2,0,2,0,1,0,2,0,0,0,0,0,0,0,2,0,1,0,2,0,2,0,1,0,2,0,0,0,\ldots)$,
(0.2) $(1,2,0,1,0,1,0,2,0,1,0,0,0,0,0,0,0,1,0,2,0,1,0,1,0,2,0,1,0,0,0,\ldots)$,

(1.0) $(1,1,0,1,0,1,2,0,2,1,1,0,1,0,1,2,2,0,2,2,0,2,0,2,1,1,0,1,1,0,1,\ldots)$,
(1.1) $(1,2,0,0,1,1,2,1,1,0,1,2,2,0,0,1,0,2,2,1,0,0,2,2,1,2,0,0,1,2,2,\ldots)$,
(1.2) $(1,0,2,2,1,1,0,1,1,2,1,0,0,2,2,1,2,0,0,1,2,2,0,0,1,0,2,2,1,0,0,\ldots)$,

(2.0) $(1,2,0,2,0,2,2,0,2,2,1,0,1,0,1,1,2,0,2,1,0,1,0,1,1,2,0,2,1,0,1,\ldots)$,
(2.1) $(1,0,2,1,1,2,0,2,1,1,1,0,0,1,2,2,2,0,0,2,2,1,0,0,1,0,2,1,1,0,0,\ldots)$,
(2.2) $(1,1,0,0,1,2,2,2,1,0,1,1,2,0,0,2,0,1,2,2,0,0,2,1,1,1,0,0,1,1,2,\ldots)$.

4 Genus one curves

In this section we consider the sequences derived from series expansion for functions on the elliptic curve

$$y^2 + xy = x^3 + x$$

over the field $\mathbf{F}_2$ of two elements. Since every point on an elliptic curve can be translated to any other, we consider only expansions around the fixed point O at infinity.

On an elliptic curve there exist no degree one functions, so Theorem 1 provides no means of constructing sequences from functions on the curve which are provably 1-perfect. However, at the end of this section we prove that certain 2-perfect sequences obtained from functions on this curve are in fact 1-perfect. In the interest of minimizing d we consider only the series expansions of non-linearly dependent functions of degree two and local parameters for O. We classify these functions as follows.

The set of rational points on E over $\mathbf{F}_2$ consists of the four points O, $(0,0)$, $(1,0)$, and $(1,1)$. Since the 2-torsion group contains only two elements, $E(\mathbf{F}_2)$ must be isomorphic to the group $\mathbf{Z}/4\mathbf{Z}$.

The automorphism $[-1]$ on E is the map $(x,y) \mapsto (x, x+y)$, which stabilizes $(0,0)$, so we identify $(0,0)$ as the 2-torsion point. Any degree two function on E which has a zero of order one at O has exactly one other zero on E, which must be one of the rational points $(0,0)$, $(1,0)$, or $(1,1)$.

The zeros and poles of functions on E satisfy an additional relation. Let $\mathrm{div}(f)$ be the divisor of the function f, and let $\mathrm{Div}_0(E, \overline{\mathbf{F}}_2)$ be the degree zero divisors defined over an algebraic closure of $\mathbf{F}_2$. Then there exists an exact sequence

$$1 \longrightarrow \overline{\mathbf{F}}_2(E)^* \longrightarrow \mathrm{Div}_0(E, \overline{\mathbf{F}}_2) \longrightarrow E(\overline{\mathbf{F}}_2) \longrightarrow 0,$$

where the first map is to take a function to its principal divisor, and the second map is the group homomorphism which takes a point divisor $[P]$ to the point P. From the exact sequence we may classify functions in $\mathbf{F}_2(E)$ by their divisors. Precisely they correspond to divisors in the kernel of the second map which are invariant under the Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_2/\mathbf{F}_2)$.

In the following table we enumerate the possible divisors of degree two functions and the function to which they correspond. In addition to the divisors of points in $E(\mathbf{F}_2)$ the two degree two divisors $\mathcal{P}$ and $\mathcal{Q}$ corresponding to the Galois invariant pairs of points in $E(\mathbf{F}_4)$ disappearing on the ideals $(x^2+x+1, y+1)$ and $(x^2+x+1, y+x+1)$ may appear.

First we determine the divisors of certain "building block" functions on E. We denote $\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f)$.

f	$\mathrm{div}_0(f)$	$\mathrm{div}_\infty(f)$
x	$2[(0,0)]$	$2[O]$
$x+1$	$[(1,0)]+[(1,1)]$	$2[O]$
y	$[(0,0)]+2[(1,0)]$	$3[O]$
$y+x$	$[(0,0)]+2[(1,1)]$	$3[O]$
$y+1$	$[(1,1)]+[\mathcal{P}]$	$3[O]$
$y+x+1$	$[(1,0)]+[\mathcal{Q}]$	$3[O]$

By enumerating all possible degree two divisors which can occur as $\mathrm{div}_\infty(f)$, we obtain the classification below of all degree two functions on E over $\mathbf{F}_2$, expressed as quotients of the functions in the previous table.

	f	$\mathrm{div}_0(f)$	$\mathrm{div}_\infty(f)$
(1)	x/y	$[O]+[(0,0)]$	$2[(0,1)]$
(2)	$x/(y+x)$	$[O]+[(0,0)]$	$2[(1,1)]$
(3)	$y/(x^2+x)$	$[O]+[(1,0)]$	$[(0,0)]+[(1,1)]$
(4)	$(x+1)/(y+1)$	$[O]+[(1,0)]$	$[\mathcal{P}]$
(5)	$(y+x)/(x^2+x)$	$[O]+[(1,1)]$	$[(0,0)]+[(1,0)]$
(6)	$(x+1)/(y+x+1)$	$[O]+[(1,1)]$	$[\mathcal{Q}]$

On the following page we give the minimal polynomial for the function f over the field $\mathbf{F}_2(t)$, where f and t are one of the above six degree two functions on $E/\mathbf{F}_2$. The entry $(i.j)$ corresponds to the pair (f,t), where f is entry (i) in the above table, and t is entry (j).

The sequence of coefficients for the series expansion of f with respect to t at O is proven to be 2-perfect by Theorem 1. For a given pair, the functions may in fact be 1-perfect. We give the experimentally determined value d_0 such that the series expansion is believed to be d_0-perfect, however this value is provably only a lower bound. The functions (1) through (6) fall in three classes which are equivalent under a linear fractional transformation. For such a pair we set d_0 equal to 0 in the table, to indicate that the corresponding sequence is periodic.

	$F(X)$	d_0
(1.1)	$X+t$	0
(1.2)	$(1+t)X+t$	0
(1.3)	$(t+t^2)X^2+(1+t)X+t$	1
(1.4)	$(1+t+t^2)X^2+(1+t)X+t$	1
(1.5)	$tX^2+(1+t)X+t+t^2$	1
(1.6)	$(1+t+t^2)X^2+(1+t)X+t+t^2$	1

	$F(X)$	d_0
(2.1)	$(1+t)X+t$	0
(2.2)	$X+t$	0
(2.3)	$tX^2+(1+t)X+t+t^2$	1
(2.4)	$(1+t+t^2)X^2+(1+t)X+t+t^2$	1
(2.5)	$(t+t^2)X^2+(1+t)X+t$	1
(2.6)	$(1+t+t^2)X^2+(1+t)X+t$	1

	$F(X)$	d_0
(3.1)	$t^2X^2+(1+t+t^2)X+t$	2
(3.2)	$X^2+(1+t+t^2)X+t$	2
(3.3)	$X+t$	0
(3.4)	$(1+t)X+t$	0
(3.5)	$tX^2+(1+t+t^2)X+t$	2
(3.6)	$(1+t+t^2)X^2+(1+t+t^2)X+t$	2

	$F(X)$	d_0
(4.1)	$t^2X^2+(1+t+t^2)X+t+t^2$	2
(4.2)	$(1+t^2)X^2+(1+t+t^2)X+t+t^2$	2
(4.3)	$(1+t)X+t$	0
(4.4)	$X+t$	0
(4.5)	$(t+t^2)X^2+(1+t+t^2)X+t+t^2$	2
(4.6)	$(1+t+t^2)X^2+(1+t+t^2)X+t+t^2$	2

	$F(X)$	d_0
(5.1)	$X^2+(1+t+t^2)X+t$	2
(5.2)	$t^2X^2+(1+t+t^2)X+t$	2
(5.3)	$tX^2+(1+t+t^2)X+t$	2
(5.4)	$(1+t+t^2)X^2+(1+t+t^2)X+t$	2
(5.5)	$X+t$	0
(5.6)	$(1+t)X+t$	0

	$F(X)$	d_0
(6.1)	$(1+t^2)X^2+(1+t+t^2)X+t+t^2$	2
(6.2)	$t^2X^2+(1+t+t^2)X+t+t^2$	2
(6.3)	$(t+t^2)X^2+(1+t+t^2)X+t+t^2$	2
(6.4)	$(1+t+t^2)X^2+(1+t+t^2)X+t+t^2$	2
(6.5)	$(1+t)X+t$	0
(6.6)	$X+t$	0

We note that due to the automorphism $[-1]$ of the curve, the nontrivial minimal polynomials appear in pairs, corresponding to function pairs which are exchanged under the automorphism induced by $[-1]$.

From the above table we note that the sequence associated to the root $f(t)$ of valuation 1 in $\mathbf{F}_2((t))$ to any of the four exceptional polynomials

$$\begin{aligned}
&(1)\ F(X) = (t+t^2)X^2 + (1+t)X + t \\
&(2)\ F(X) = (1+t+t^2)X^2 + (1+t)X + t \\
&(3)\ F(X) = tX^2 + (1+t)X + t + t^2 \\
&(4)\ F(X) = (1+t+t^2)X^2 + (1+t)X + t + t^2
\end{aligned}$$

over $\mathbf{F}_2(t)$, were observed to exhibit a 1-perfect complexity profile. The sequences associated with the roots of above four polynomials are:

$$\begin{aligned}
&(1)\ (1,1,0,1,0,1,1,1,0,1,1,1,0,1,0,1,0,1,1,1,0,1,0,1,0,1,1,1,0,1,1,1,\ldots), \\
&(2)\ (1,0,1,0,0,1,0,1,1,1,1,0,1,0,0,1,0,0,1,1,0,0,1,0,0,1,0,1,1,1,1,0,\ldots), \\
&(3)\ (1,0,1,1,1,1,0,0,1,1,0,0,1,1,1,1,1,1,0,0,1,1,1,1,1,1,0,0,1,1,0,0,\ldots), \\
&(4)\ (1,1,0,0,1,0,0,0,0,1,0,1,1,1,1,1,1,1,1,0,1,0,0,1,0,0,1,1,0,0,1,1,\ldots).
\end{aligned}$$

In particular we note that the above four sequences are different from the 1-perfect binary sequences in Section 3.

The following theorem of Wang and Massey [7] (see Niederreiter [2]) characterizes all binary perfect sequences.

Theorem 3. *A sequence* $(1, a_2, a_3 \ldots)$ *over the binary field is* 1*-perfect if and only if* $a_n + a_{2n} + a_{2n+1} = 0$.

In terms of a series $f(t) = t + a_2t^2 + a_3t^3 + \cdots$ we easily check that the coefficient of t^{2n+1} in

$$t\,f(t)^2 + (1+t)f(t) + t$$

is $a_n + a_{2n} + a_{2n+1}$ for all $n \geq 1$. Taking the derivative with respect to t, gives the following corollary.

Corollary 1. *A series* $f(t) = t + a_2t^2 + a_3t^3 + \cdots$ *is* 1*-perfect if and only if it satisfies the differential equation*

$$(1+t)\frac{df}{dt}(t) = f(t)^2 + f(t) + 1.$$

By Corollary 1, it follows immediately that roots $f(t)$ of the four exceptional polynomials are 1-perfect. For the first polynomial, we have

$$F(f(t)) = (t+t^2)f(t)^2 + (1+t)f(t) + t = 0.$$

Taking the first derivative, we obtain the characterizing differential equation for binary perfect sequences. For each of the other polynomials we obtain the same derivative, proving that the corresponding series are 1-perfect as experimentally observed.

The preceeding corollary allows us to determine whether a function $f(t)$ is 1-perfect by differentiating its minimal polynomial over $\mathbf{F}_2((t))$. The following corollary gives an alternative algebraic characterization of $f(t)$.

Corollary 2. *Every binary 1-perfect series* $f(t) = t + a_2t^2 + a_3t^3 + \cdots$ *can be uniquely written in the form* $f(t) = v^2 + t\,u^2$ *where* u *lies in* $1 + t\,\mathbf{F}_2[[t]]$ *and* v *is the root of*

$$v^2 + v = 1 + u + t\,u^2,$$

lying in $t\,\mathbf{F}[[t]]$. *The series* u *and* v *are uniquely defined by* $f(t)$ *and conversely every* u *in* $1 + t\,\mathbf{F}_2[[t]]$ *gives rise to a unique solution* v *in* $t\,\mathbf{F}_2[[t]]$ *such that* $f(t) = v^2 + t\,u^2$ *is 1-perfect.*

Proof. Every $f(t)$ in $\mathbf{F}_2[[t]]$ can be written in the form $f(t) = v^2 + t\,u^2$. The leading term is t if and only if u lies in $1 + t\,\mathbf{F}_2[[t]]$ and v in $t\,\mathbf{F}_2[[t]]$, and one verifies that $df/dt = u^2$. By Corollary 1, the series $f(t)$ is 1-perfect if and only if

$$(1 + t)\frac{df}{dt} = f^2 + f + 1.$$

After a substitution and rearrangement, this is equivalent to $(v^2 + v + 1 + u + t\,u^2)^2 = 0$. Since $\mathbf{F}_2((t))$ is a field, the results follows. □

A binary 1-perfect sequence $f(t)$ arises as the series expansion with respect to t of a function on a curve $\mathcal{X}$ if and only if u is algebraic over $\mathbf{F}_2(t)$. The function t has degree 2 on $\mathcal{X}$ as in Theorem 1 if and only if exactly one of u or v is a rational function in t. If u is transcendental over $\mathbf{F}_2(t)$ then the $\mathbf{F}_2(u, t)$ is the function field of the projective plane, and $f(t)$ gives a function on a quadratic surface covering the plane.

References

1. Lang, S. *Algebraic Number Theory.* Second Edition. Graduate Texts in Mathematics, **110**. Springer-Verlag, New York, 1994.
2. Niederreiter, H. "Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences." in *Contributions to General Algebra 5* (Salzburg, 1986), 221–233, Hölder-Pichler-Tempsky, Vienna, 1987.
3. Niederreiter, H. "Sequences with almost perfect linear complexity profile," in *Advances in Cryptology–EUROCRYPT '87*, D. Chaum and W. L. Price, eds. Springer-Verlag, Berlin: Lecture Notes in Computer Science, vol. 304, 1988, pp.37-51.
4. Rueppel, R. A. *Analysis and Design of Stream Ciphers.* Communication and Control Engineering Series. Springer-Verlag, Berlin-New York, 1986.
5. Rueppel, R. A. "Stream ciphers," in *Contemporary Cryptology–The Science of Information Integrity*, G. J. Simmons, Ed., 65–134, IEEE, New York, 1992.
6. Silverman, J. H. *The arithmetic of ellitic curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York, 1986.
7. Wang, M.-Z. and Massey, J. L. *The characterization of all binary sequences with a perfect linear complexity profile,* Paper presented at *EUROCRYPT '86*, Linköping, 1986.
8. C. P. Xing and K. Y. Lam, *Sequences with almost perfect linear complexity profiles and curves over finite fields,* To appear in *IEEE Trans. Inform. Theory.*
9. C. P. Xing, H. Niederreiter, K. Y. Lam and C. S. Ding, *Constructions of sequences with almost perfect linear complexity profiles from curves over finite fields*, Preprint, 1998.