COMMUNICATIONS IN MATHEMATICS

VOLUME
22/2014
No. 2

ISSN 1804-1388 (Print)
ISSN 2336-1298 (Online)

Available online at
http://cm.osu.cz

UNIVERSITAS OSTRAVIENSIS

Communications in Mathematics 22 (2014) 151–157

On a binary recurrent sequence of polynomials

Reinhardt Euler, Luis H. Gallardo, Florian Luca

Abstract. In this paper, we study the properties of the sequence of polynomials given by $g_0 = 0,\ g_1 = 1,\ g_{n+1} = g_n + \Delta g_{n-1}$ for $n \geq 1$, where $\Delta \in \mathbb{F}_q[t]$ is non-constant and the characteristic of $\mathbb{F}_q$ is 2. This complements some results from [2].

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = 2^k$ elements for some $k \geq 1$. Given $\Delta \in \mathbb{F}_q[t]$ non constant define $\{g_n\}_{n\geq 0}$ by $g_0 = 0,\ g_1 = 1$ and

$$g_{n+2} = g_{n+1} + \Delta g_n \quad \text{for} \quad n \geq 0\,. \tag{1}$$

This sequence was studied in [2]. In this paper, we correct an oversight from [2], answer an open question about this sequence asked there and prove a few more properties of this sequence.

In [2], it was shown that $g_n = 0$ holds infinitely often. Here, we correct this statement and show that in fact $g_n = 1$ holds infinitely often and $g_n = 0$ for $n = 0$ only. At the end of [2] it was asked whether the sequence $\{g_n\}_{n\geq 0}$ is periodic. Here, we show that this is not the case by proving in fact that $\limsup_{n\to\infty} \deg(g_n) = \infty$. We also find explicit formulas for g_n when $n = 2^m,\ 2^m - 1,\ 2^m + 1$ for some $m \geq 0$. We also find more properties of the polynomials $\{g_n\}_{n\geq 0}$. For example, it is easy to show by induction that the degree of g_n is at most $n-1$ and that g_n is a polynomial in Δ with coefficients in $\{0,1\}$. We let $\ell(g_n)$ be the *length* of g_n as a polynomial in $\mathbb{F}_q[\Delta]$, namely the sum of its coefficients and compute this number. We find that $\ell(g_n) = a_n$, where $\{a_n\}_{n\geq 0}$ is the Stern-Brocot sequence given by $a_0 = 0,\ a_1 = 1$ and

$$a_{2n} = a_n \qquad \text{and} \qquad a_{2n+1} = a_{n+1} + a_n \qquad \text{for all} \qquad n \geq 0\,.$$

We also compute how many of the a_n monomials in g_n have odd degree in Δ. Let b_n be this number. We find that $b_{2n} = 0$ and $b_{2n+1} = a_n$ for all $n \geq 0$.

2010 MSC: 11T55, 11T06, 11B39
Key words: sequences of binary polynomials, Stern-Brocot sequence, perfect fields of characteristic 2

All these results are summarized in the theorem below.

Theorem 1. *The following holds:*

(i) $g_{2^m} = 1$ *for all* $m \geq 0$,

(ii) $g_{2^m+1} = 1 + \Delta + \Delta^2 + \cdots + \Delta^{2^{m-1}}$ *for all* $m \geq 1$,

(iii) $g_{2^m-1} = 1 + \Delta + \Delta^3 + \cdots + \Delta^{2^{m-1}-1}$ *for all* $m \geq 1$,

(iv) $\ell(g_n) = a_n$,

(v) $b_{2n} = 0$,

(vi) $b_{2n+1} = a_n$ *for all* $n \geq 0$.

2 The proof of Theorem 1

We first prove a lemma.

Lemma 1. *For all* $n \geq 0$*:*

(i) $g_{2n+4} = g_{2n+2} + \Delta^2 g_{2n}$,

(ii) $g_{2n} = g_n^2$.

Proof. For (i), we write using (1) (with n replaced by $2n$ and by $2n+2$) and the fact that the characteristic of $\mathbb{F}_q$ is 2:

$$g_{2n+1} = g_{2n+2} + \Delta g_{2n} \qquad \text{and} \qquad g_{2n+3} = g_{2n+4} + \Delta g_{2n+2} . \tag{2}$$

Inserting the above relations into (1) with n replaced by $2n+1$, we get

$$g_{2n+4} + \Delta g_{2n+2} = g_{2n+3} = g_{2n+2} + \Delta g_{2n+1} = g_{2n+2} + \Delta(g_{2n+2} + \Delta g_{2n}) ,$$

or

$$g_{2n+4} = g_{2n+2} + \Delta^2 g_{2n}$$

as desired. For (ii), we use induction on n. The cases $n = 0, 1$ are clear. Assuming that $n \geq 2$ and that (ii) holds for all $m \leq n$, we have, by (i),

$$g_{2n+2} = g_{2n} + \Delta^2 g_{2n-2} = g_n^2 + \Delta^2 g_{n-1}^2 = (g_n + \Delta g_{n-1})^2 = g_{n+1}^2 ,$$

which completes the induction and the proof of (ii). □

We are now ready to prove Theorem 1. We first prove (i)–(iii) by induction on $m \geq 0$. The cases $m = 0, 1$ can be verified by hand. Assume that $m \geq 2$ and (i)–(iii) hold for all $n < m$. Then, by Lemma 1 (ii) and the induction hypothesis, we have

$$g_{2^m} = (g_{2^{m-1}})^2 = 1^2 = 1 .$$

Further,

$$1 = g_{2^m} = g_{2^m-1} + \Delta g_{2^m-2} = g_{2^m-1} + \Delta(g_{2^{m-1}-1})^2,$$

so

$$\begin{aligned} g_{2^m-1} &= 1 + \Delta g_{2^{m-1}-1}^2 \\ &= 1 + \Delta(1 + \Delta + \Delta^3 + \cdots + \Delta^{2^{m-2}-1})^2 \\ &= 1 + \Delta + \Delta^3 + \cdots + \Delta^{2^{m-1}-1}. \end{aligned}$$

Finally,

$$\begin{aligned} g_{2^m+1} &= g_{2^m} + \Delta g_{2^m-1} \\ &= 1 + \Delta(1 + \Delta + \Delta^3 + \cdots + \Delta^{2^{m-1}-1}) \\ &= 1 + \Delta + \Delta^2 + \cdots + \Delta^{2^{m-1}}. \end{aligned}$$

For (iv), we check that the statement is true for $n = 0, 1$. Since

$$g_{2n} = g_n^2$$

we have $a_{2n} = \ell(g_{2n}) = \ell(g_n^2) = \ell(g_n) = a_n$. Since

$$g_{2n+1} = g_{2n+2} + \Delta g_{2n} = g_{n+1}^2 + \Delta g_n^2 \tag{3}$$

and every monomial appearing in either g_{n+1}^2 or g_n^2 appears with even degree, we have that

$$\ell(g_{2n+1}) = \ell(g_{n+1}^2) + \ell(g_n^2) = \ell(g_{n+1}) + \ell(g_n) = a_{n+1} + a_n\,,$$

which is what we wanted.

We now prove (v) and (vi). By (ii) of Lemma 1, we have that

$$g_{2n} = g_n^2$$

is a polynomial in Δ whose monomials have even degree. Hence, $b_{2n} = 0$. For the odd n, note that $b_n = \ell(g_n')$, where g_n' denotes the derivative of g_n as a polynomial in Δ. Taking the derivative in relation (1) and using the fact that the characteristic of $\mathbb{F}_q$ is 2, we get

$$g_n = g_{n+2}' + g_{n+1}' + \Delta g_n'\,.$$

Inserting the above relation with n replaced by $n+1$ and $n+2$ in (1), we get

$$\begin{aligned} g_{n+4}' + g_{n+3}' + \Delta g_{n+2}' &= g_{n+2} = g_{n+1} + \Delta g_n \\ &= g_{n+3}' + g_{n+2}' + \Delta g_{n+1}' + \Delta(g_{n+2}' + g_{n+1}' + \Delta g_n')\,, \end{aligned}$$

which leads to

$$g_{n+4}' = g_{n+2}' + \Delta^2 g_n'\,.$$

Since $g_0 = 0,\ g_1 = 1,\ g_2 = 1,\ g_3 = 1 + \Delta$, we have that $g_1' = 0$ and $g_3' = 1$. Thus, we get that $g_{2n+1}' = g_n(\Delta^2)$, where $g_n(\Delta^2)$ is the same sequence of polynomials $\{g_n\}_{n\geq 0}$ but with Δ replaced by Δ^2. Now (vi) follows from (iv).

A simpler argument for (vi) suggested by the referee goes as follows: since

$$g_{n+1}^2 = g_{2n+2} = g_{2n+1} + \Delta g_{2n} = g_{2n+1} + \Delta g_n^2\,,$$

taking derivatives yields

$$0 = (g_{n+1}^2)' = g'_{2n+1} + g_n^2 + \Delta(g_n^2)' = g'_{2n+1} + g_n^2\,,$$

and therefore $g'_{2n+1} = g_{2n}$. Hence,

$$b_{2n+1} = \ell(g'_{2n+1}) = \ell(g_{2n}) = a_{2n} = a_n\,.$$

Of course, the even case can be treated similarly:

$$b_{2n} = \ell(g'_{2n}) = \ell((g_n^2)') = \ell(0) = 0\,.$$

Remark 1. Another approach to (iv)–(vi) of Theorem 1 due to the referee is as follows. First let us define the sequence $\{g_n\}_{n\geq 0}$ of polynomials in $\mathbb{Z}[\Delta]$ given by the same recurrence

$$g_{n+2} = g_{n+1} + \Delta g_n$$

with $g_0 = 0$, $g_1 = 1$. Then we have the following representation of the general term g_n.

Lemma 2. *We have for $n \geq 0$,*

$$g_{n+1} = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} \Delta^k. \tag{4}$$

Proof. For $n = 0, 1$, we have $g_1 = 1$, $g_2 = 1 + \Delta$ which are consistent with what is shown at (4) when $n = 0, 1$. Assuming now that $n \geq 1$ and that (4) holds both for n and for n replaced by $n - 1$, then

$$\begin{aligned} g_{n+2} &= g_{n+1} + \Delta g_n \qquad\qquad (5)\\ &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} \Delta^k + \Delta \left(\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} \Delta^k \right) \\ &= \binom{n}{0} + \sum_{k=1}^{\lfloor n/2 \rfloor} \left(\binom{n-k}{k} + \binom{(n-1)-(k-1)}{k-1} \right) \Delta^k \\ &\quad + \sum_{k=\lfloor n/2 \rfloor + 1}^{\lfloor (n-1)/2 \rfloor + 1} \binom{n-1-(k-1)}{k-1} \Delta^k \\ &= 1 + \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n+1-k}{k} \Delta^k + \sum_{k=\lfloor n/2 \rfloor + 1}^{\lfloor (n-1)/2 \rfloor + 1} \binom{n-k}{k-1} \Delta^k. \qquad (6) \end{aligned}$$

In the above formula we used the fact that

$$\binom{n-k}{k}+\binom{(n-1)-(k-1)}{k-1}=\binom{n-k}{k}+\binom{n-k}{k-1}=\binom{n+1-k)}{k}.$$

The left-most term 1 in (5) equals $\binom{n+1-0}{0}$, the last term is 0 when n is even because then $\lfloor n/2\rfloor=\lfloor (n-1)/2\rfloor+1=\lfloor (n+1)/2\rfloor$, while in case when $n=2m+1$ is odd, then the last term is the monomial in $k=m+1=\lfloor (n+1)/2\rfloor$ with coefficient $\binom{2m-m}{m}=1=\binom{n+1-k}{k}$. This completes the induction. □

By Lemma 2, we have, in characteristic 2,

$$g_{n+1}=\sum_{k=0}^{\lfloor n/2\rfloor}\left[\binom{n-k}{k} \bmod 2\right]\Delta^k. \tag{7}$$

Hence,

$$\ell(g_{n+1})=\sum_{k=0}^{\lfloor n/2\rfloor}\left[\binom{n-k}{k} \bmod 2\right]=a_{n+1}\,,$$

which is (iv) for all $n\ge 1$ (the fact that $\ell(g_0)=a_0=0$ is clear). The last equality is Theorem 4.1 in [4] (see also sequence A002487 in [5]). Letting

$$b_{n+1}:=\sum_{\substack{k=0\\ k \text{ odd}}}^{\lfloor n/2\rfloor}\left[\binom{n-k}{k} \bmod 2\right],$$

we have, since $\binom{\text{even}}{\text{odd}}=\text{even}$ (which can be easily checked by invoking Lucas' theorem on binomial coefficients modulo p for the prime $p=2$), we get

$$b_{2n}:=\sum_{\substack{k=0\\ k \text{ odd}}}^{\lfloor n/2\rfloor}\left[\binom{2n-k-1}{k} \pmod 2\right]=0\,,$$

which is (v). Further, because $\binom{2n}{2k}\equiv\binom{n}{k} \bmod 2$ (again by Lucas's theorem), we have

$$\begin{aligned} a_{2n+1}-b_{2n+1}&=\sum_{k=0}^{n}\left[\binom{2n-2k}{2k} \bmod 2\right]=\sum_{k=0}^{n}\left[\binom{n-k}{k} \bmod 2\right]\\ &=a_{n+1}\,, \end{aligned}$$

from where we get that $b_{2n+1}=a_{2n+1}-a_{n+1}=a_n$, which is (vi).

3 Comments and Open questions

First of all, observe that our results hold more generally for the finite field $\mathbb{F}_q$, with q even, replaced by any infinite field of characteristic 2, since we have not used the property $h^q = h$ for the elements h of our field. There are many questions one can ask about the sequence $\{g_n\}_{n\geq 0}$. For example, what can we say about the number of irreducible factors of g_n as a polynomial in Δ? Is it true that all roots of g_{2n+1} are simple? We leave such questions to the reader. As for the degree of g_n, writing $n = 2^a b$, where b is odd, gives $\deg(g_n) = 2^a(b-1)/2$. One may recognize this last quantity as $n * (n-1)/2$, where for nonnegative integers m and n, the quantity $m * n$ denotes the nonnegative integer whose binary representation is the bitwise AND operation of the binary representations of m and n. Indeed, since $g_{2n} = g_n^2$, we get that $g_n = g_{2^a b} = g_b^{2^a}$, so it suffices to show that if m is odd, then g_m has degree $(m-1)/2$. But this follows by replacing n by $m-1$ in (7):

$$g_m = \sum_{k=0}^{(m-1)/2} \left[\binom{m-1-k}{k} \bmod 2 \right] \Delta^k,$$

and noting that the last term of the above sum corresponding to $k = (m-1)/2$ has coefficient $\binom{(m-1)/2}{(m-1)/2} = 1$.

The above questions may be asked in the more general context of the field $\mathbb{F}[\Delta]$. A restriction to perfect fields of characteristic 2 may be useful since then we have for all polynomials $C \in \mathbb{F}[t]$ the simple relation

$$C = A^2 + tB^2$$

for some polynomials $A, B \in \mathbb{F}[t]$. By construction, the elements of our sequence with odd subscripts satisfy a relation of this type (see (3) in the proof of (iv)).

Observe also that this sequence can be easily dealt with over fields of characteristic $p > 2$ by the Binet formulae. However, in our case $p = 2$ and $\mathbb{F}$ finite, we were not able to use these formulae to describe our sequence since we do not know explicitly the solutions of the quadratic equation

$$x^2 + x + \Delta = 0$$

in the ring $\mathbb{F}_q[t]$. This motivates our new approach to study the sequence in the present paper.

Moreover, the reader may try to check which of the properties in [3], that hold for the classical case in which the coefficients are integers, are still true in our characteristic 2 case by using the tools of [1].

4 Acknowledgements

We thank the referee for comments which improved the quality of our paper and for providing proofs to some of our results which are alternative to our original ones. This paper was written during a visit of F. L. at the Mathematics Department of the Université de Bretagne Occidentale in Brest in February, 2014. He thanks the people of this institution for their hospitality. During the preparation of this paper, F. L. was also supported in part by Project PAPIIT IN104512 (UNAM).

References

[1] J. Cherly, L. Gallardo, L. Vaserstein, E. Wheland: Solving quadratic equations over polynomial rings of characteristic two. *Publ. Math.* 42 (1998) 131–142.

[2] R. Euler, L.H. Gallardo: On explicit formulae and linear recurrent sequences. *Acta Math. Univ. Comenianae* 80 (2011) 213–219.

[3] T.-X. He, P.J.-S. Shiue: On sequences of numbers and polynomials defined by linear recurrence relations of order 2. Art. ID 709386, 21 pp.

[4] S. Northshield: Stern's diatomic sequence $0, 1, 1, 2, 1, 3, 2, 3, 1, 4, \dots$. *Amer. Math. Monthly* 117 (2010) 581–598.

[5] N.J.A. Sloane: OEIS. https://oeis.org/

Authors' addresses:

Reinhardt Euler: Lab-STICC UMR CNRS 6285, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest, Cedex 3, France

E-mail: Reinhardt.Euler@univ-brest.fr

Luis H. Gallardo: Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest, Cedex 3, France

E-mail: Luis.Gallardo@univ-brest.fr, gallardo@math.cnrs.fr

Florian Luca: Mathematical Institute, UNAM Juriquilla, 76230 Santiago de Querétaro, México, and School of Mathematics, University of the Witwatersrand, P. O. Box Wits 2050, South Africa

E-mail: fluca@matmor.unam.mx

Received: 9 September, 2014
Accepted for publication: 27 November, 2014
Communicated by: Karl Dilcher