#A50 INTEGERS 15 (2015)

FACTORS AND IRREDUCIBILITY OF GENERALIZED STERN POLYNOMIALS

Karl Dilcher[1]
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, Canada
dilcher@mathstat.dal.ca

Larry Ericksen
P.O. Box 172, Millville, NJ 08332-0172, USA
LE22@cornell.edu

Received: 1/14/15, Revised: 7/7/15, Accepted: 11/15/15, Published: 12/11/15

Abstract

We investigate an infinite class of polynomial sequences $a_t(n;z)$ with integer parameter $t \geq 1$, which reduce to the well-known Stern (diatomic) sequence when $z = 1$ and are $(0,1)$-polynomials when $t \geq 2$. These sequences are related to the theory of hyperbinary expansions. The main purpose of this paper is to obtain various irreducibility and factorization results, most of which involve cyclotomic polynomials.

1. Introduction

The *Stern sequence*, also known as *Stern's diatomic sequence*, is one of the most remarkable integer sequences in number theory and combinatorics. Using the notation $\{a(n)\}_{n\geq 0}$, it can be defined by $a(0) = 0$, $a(1) = 1$, and for $n \geq 1$ by

$$a(2n) = a(n), \qquad a(2n+1) = a(n) + a(n+1). \tag{1.1}$$

Numerous properties and references can be found, e.g., in [16, A002487] or [18]. The most remarkable properties are the following: The quotients $a(n)/a(n+1), n \geq 1$, give an enumeration without repetitions of all the positive rationals; and $a(n+1)$ gives the number of hyperbinary expansions of n (see, e.g., [2]).

The current paper deals with the following generalization of the Stern polynomials of [6], recently introduced by the authors in [5] in connection with a complete

[1]Supported in part by the Natural Sciences and Engineering Research Council of Canada.

characterization of hyperbinary expansions. Given an integer $t \geq 1$, we define $a_t(0; z) = 0$, $a_t(1; z) = 1$, and for $n \geq 1$ we let

$$a_t(2n; z) = a_t(n; z^t), \tag{1.2}$$
$$a_t(2n+1; z) = z\, a_t(n; z^t) + a_t(n+1; z^t). \tag{1.3}$$

For $t = 2$ this definition reduces to that of the polynomials of [6] (see also [3] and [7]). Polynomials closely related to $a_1(n; z)$ were studied in [1] and [20], and generalizations of $a_1(n; z)$ and related sequences were considered in [13] and [14].

Comparing (1.2) and (1.3) with (1.1), we immediately see that for all integers $t \geq 1$ and $n \geq 1$ we have

$$a_t(n; 0) = 1, \qquad a_t(n; 1) = a(n), \tag{1.4}$$

and by iterating (1.2) and considering (1.3) we see that

$$a_t(n; z) = 1 \quad \text{if and only if} \quad n = 2^m, \quad m \geq 0. \tag{1.5}$$

The first polynomials $a_t(n; z)$, for $n \leq 20$, are listed in Table 1.

n	$a_t(n;z)$	n	$a_t(n;z)$
1	1	11	$1+z+z^{t+1}+z^{t^2}+z^{t^2+1}$
2	1	12	$1+z^{t^2}$
3	$1+z$	13	$1+z+z^t+z^{t^2+1}+z^{t^2+t}$
4	1	14	$1+z^t+z^{t^2+t}$
5	$1+z+z^t$	15	$1+z+z^{t+1}+z^{t^2+t+1}$
6	$1+z^t$	16	1
7	$1+z+z^{t+1}$	17	$1+z+z^t+z^{t^2}+z^{t^3}$
8	1	18	$1+z^t+z^{t^2}+z^{t^3}$
9	$1+z+z^t+z^{t^2}$	19	$1+z+z^{t+1}+z^{t^2}+z^{t^2+1}+z^{t^3}+z^{t^3+1}$
10	$1+z^t+z^{t^2}$	20	$1+z^{t^2}+z^{t^3}$

Table 1: $a_t(n; z)$, $1 \leq n \leq 20$.

Table 1 indicates that each $a_t(n; z)$ is a $(0, 1)$-polynomials in z, and that the exponents of z are $(0, 1)$-polynomials in t. These facts, and other results on the structure of the polynomials $a_t(n; z)$, were proved in [5].

The present paper deals with the question of reducibility and irreducibility of the polynomials $a_t(n; z)$, including explicit factorizations in some cases. Section 2 is devoted to "short polynomials," namely those with two to five terms. In Section 3 we use a classical result of Lazarus Fuchs to obtain factorizations of an auxiliary polynomial sequence. This is then applied to some of the results in Section 4, where we study two particular classes of generalized Stern polynomials with increasing numbers of terms. In Section 5, we address the question of multiple roots of these last two classes of polynomials, and we conclude the paper with a few further remarks in Section 6.

2. Short Polynomials

In [3] we investigated reducibility and irreducibility of the Stern polynomials $a_2(n;z)$ of 2, 3, and 4 terms. In this section we will extend these results to all binomials, trinomials and quadrinomials among the generalized Stern polynomials $a_t(n;z)$, and in addition we will prove some results on pentanomials. As we did in [3], we use the following result of Stern [21, p. 202] (see also [12]): *Given an integer $k \geq 2$, the number of integers n in the interval $2^{k-1} \leq n \leq 2^k$ for which $a(n) = k$ is $\varphi(k)$, where φ denotes Euler's totient function. Furthermore, it is the same number in any subsequent interval between two consecutive powers of* 2. Since for $t \geq 2$ the $a_t(n;z)$ are $(0,1)$-polynomials, by (1.4) and (1.2) this means that we can explicitly write down all binomials, trinomials, quadrinomials and pentanomials among the $a_t(n;z)$ for $t \geq 2$, of which there are $\varphi(2) + \cdots + \varphi(5) = 9$ different classes. We will deal with them in sequence.

2.1. Binomials

Since $a_t(3;z) = 1 + z$ for all $t \geq 1$, by (1.2) all binomials are given by

$$a_t(3 \cdot 2^k; z) = 1 + z^{t^k}. \tag{2.1}$$

For $k = 0$ this is trivially irreducible.

Proposition 2.1. *For $k \geq 1$ the binomial $a_t(3 \cdot 2^k; z)$ is irreducible if and only if $t \geq 1$ is a power of* 2.

Proof. When $t = 1$, this is trivially true, so let $t \geq 2$. Using a well-known argument, we note that if t is not a power of 2, then $t = uv$ with $v \geq 3$ odd. Then by (2.1),

$$a_t(3 \cdot 2^k; z) = 1 + \left(z^{u^k v^{k-1}}\right)^v = (1+y)(1 - y + y^2 - \cdots + y^{v-1}),$$

where $y := z^{u^k v^{k-1}}$. This gives a nontrivial factorization. On the other hand, when $t = 2^\nu$ for an integer $\nu \geq 1$, then we have

$$a_t(3 \cdot 2^k; z) = 1 + z^{2^{\nu k}} = \Phi_{2^{\nu k + 1}}(z)$$

which, as a cyclotomic polynomial, is irreducible. □

2.2. Trinomials

We see from Table 1 that the two trinomials between $n = 4$ and $n = 8$ are

$$a_t(5; z) = 1 + z + z^t, \qquad a_t(7; z) = 1 + z + z^{t+1},$$

which means that all generalized Stern trinomials are given by

$$a_t(5 \cdot 2^k; z) = 1 + z^{t^k} + z^{t^{k+1}} = 1 + \left(z^{t^k}\right) + \left(z^{t^k}\right)^t, \tag{2.2}$$

$$a_t(7 \cdot 2^k; z) = 1 + z^{t^k} + z^{(t+1)t^k} = 1 + \left(z^{t^k}\right) + \left(z^{t^k}\right)^{t+1}. \tag{2.3}$$

When $t = 1$, we see that both polynomials, $1 + 2z$ and $1 + z + z^2$, respectively, are irreducible. We therefore assume that $t \geq 2$.

Proposition 2.2. *Let $k \geq 0$ and $t \geq 2$ be integers.*

(a) If $t \equiv 0, 1 \pmod 3$, then $a_t(5 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 2 \pmod 3$, we have $(z^2 + z + 1) \mid a_t(5 \cdot 2^k; z)$; that is, $a_t(5 \cdot 2^k; z)$ is reducible in this case, with the exception of $a_2(5; z) = z^2 + z + 1$.

Proof. By a theorem of Selmer [19, Theorem 1], $1 + z + z^t$ is irreducible when $t \equiv 0, 1 \pmod 3$, but is divisible by $1 + z + z^2$ when $t \equiv 2 \pmod 3$. By a theorem of Tverberg [22], a trinomial of the type $z^n \pm z^m \pm 1$ is irreducible if it has no zero of modulus 1. If it does have zeros of modulus 1, they can be collected to give a rational factor. Now, since z^{t^k} has modulus 1 if and only if z does, the polynomial $a_t(5 \cdot 2^k; z)$ in (2.2) has the same property as does $1 + z + z^t$, which corresponds to the case $k = 0$. Finally, the exceptional case $a_2(5; z)$ comes from $z^2 + z + 1$ being its own irreducible factor. □

Proposition 2.3. *Let $k \geq 0$ and $t \geq 2$ be integers.*

(a) If $t \equiv 0, 2 \pmod 3$, then $a_t(7 \cdot 2^k; z)$ is irreducible.

(b) If $t \equiv 1 \pmod 3$, we have $(z^2 + z + 1) \mid a_t(7 \cdot 2^k; z)$; that is, $a_t(7 \cdot 2^k; z)$ is reducible in this case.

The proof of this result is completely analogous to that of Proposition 2.2, applying the theorems of Selmer and Tverberg to (2.3).

2.3. Quadrinomials

We see from Table 1 that the two quadrinomials between $n = 8$ and $n = 16$ are

$$a_t(9; z) = 1 + z + z^t + z^{t^2}, \qquad a_t(15; z) = 1 + z + z^{t+1} + z^{t^2+t+1},$$

and accordingly, all generalized Stern quadrinomials are given by

$$a_t(9\cdot 2^k;z) = 1+z^{t^k}+z^{t^{k+1}}+z^{t^{k+2}}, \tag{2.4}$$
$$a_t(15\cdot 2^k;z) = 1+z^{t^k}+z^{(t+1)t^k}+z^{(t^2+t+1)t^k}. \tag{2.5}$$

Once again, we treat the case $t=1$ separately, noting that $a_1(9\cdot 2^k;z)=1+3z$, which is trivially irreducible, while $a_1(15\cdot 2^k;z)=1+z+z^2+z^3=(1+z)(1+z^2)$.

To deal with the quadrinomials in (2.4) and (2.5) for $t\geq 2$, we use the following theorem of Finch and Jones [9]:

The polynomial $x^a+x^b+x^c+1$ is reducible if and only if exactly one of the integers $a/2^\nu, b/2^\nu, c/2^\nu$ is even, where $\gcd(a,b,c)=2^\nu m$ with m odd.

We are now ready to state and prove the next two results.

Proposition 2.4. *For all integers $k\geq 0$ and $t\geq 2$, the quadrinomial $a_t(9\cdot 2^k;z)$ is irreducible.*

Proof. We use the theorem of Finch and Jones with $a=t^k$, $b=t^{k+1}$, $c=t^{k+2}$. If t is odd, then $\nu=0$ and all three of a,b,c are odd.

If t is even, set $t=2^\mu u$ with u odd. Then

$$a=2^{k\mu}u^k,\quad b=2^{(k+1)\mu}u^{k+1},\quad c=2^{(k+2)\mu}u^{k+2}.$$

So $\gcd(a,b,c)=2^{k\mu}u^k$, and $a/2^{k\mu}$ is odd while $b/2^{k\mu}$ and $c/2^{k\mu}$ are even. Hence in both cases $a_t(9\cdot 2^k;z)$ is irreducible. □

Proposition 2.5. *Let $k\geq 0$ and $t\geq 2$ be integers.*

(a) If t is even then $a_t(15\cdot 2^k;z)$ is irreducible.

(b) If t is odd then $a_t(15\cdot 2^k;z)$ is divisible by $1+z^{t^k}$.

Proof. In view of (2.5) we apply the theorem of Finch and Jones with $a=t^k$, $b=(t+1)t^k$, $c=(t^2+t+1)t^k$. If t is even, say $t=2^\mu u$ with u odd, then all three of $a/2^{k\mu}$, $b/2^{k\mu}$, $c/2^{k\mu}$ are odd, which means that $a_t(15\cdot 2^k;z)$ is irreducible.

If t is odd then clearly a and c are odd, while b is even. But also, if we rewrite

$$a_t(15\cdot 2^k;z) = 1+\left(z^{t^k}\right)+\left(z^{t^k}\right)^{t+1}+\left(z^{t^k}\right)^{t^2+t+1},$$

it is obvious that it vanishes for $z^{t^k}=-1$ when t is odd. □

2.4. Pentanomials

In the case of pentanomials, i.e., polynomials with five terms, there do not seem to exist suitable irreducibility results (over $\mathbb{Q}$) in the literature. This is perhaps not surprising, as the authors of [9] and [19] remark on the tedium and complexity of obtaining results on quadrinomial. In this subsection we will therefore state only some reducibility results which follow from more general results in the next section.

The four principal pentanomials among the generalized Stern polynomials are easily identified as

$$\begin{aligned}
a_t(11;z) &= 1 + z + z^{t+1} + z^{t^2} + z^{t^2+1},\\
a_t(13;z) &= 1 + z + z^{t} + z^{t^2+1} + z^{t^2+t},\\
a_t(17;z) &= 1 + z + z^{t} + z^{t^2} + z^{t^3},\\
a_t(31;z) &= 1 + z + z^{t+1} + z^{t^2+t+1} + z^{t^3+t^2+t+1};
\end{aligned}$$

for the first three see Table 1. Note that this list does not contradict Stern's result quoted at the beginning of this section since $a_t(22;z) = a_t(11;z^t)$ and $a_t(26;z) = a_t(13;z^t)$ are also pentanomials when $t \geq 2$, for a total of four in the interval $2^4 \leq n \leq 2^5$.

In the result below we make use of the fact that for a prime p the pth cyclotomic polynomial is

$$\Phi_p(z) = 1 + z + z^2 + \cdots + z^{p-1}.$$

Proposition 2.6. *Let $t \geq 2$ be an integer.*

(a) If $t \equiv 2, 3 \pmod 5$, then $\Phi_5(z)$ divides $a_t(17;z)$.

(b) If $t \equiv 1 \pmod 5$, then $\Phi_5(z)$ divides $a_t(31;z)$.

Both parts are direct consequences of Propositions 3.1 and 3.2, respectively. We observed that $a_t(17;z)$ and $a_t(31;z)$ appear to be irreducible in the remaining residue classes for t, and that $a_t(11;z)$ and $a_t(13;z)$ appear to be irreducible for all $t \geq 2$.

Finally, for the sake of completeness we mention that $a_1(11;z) = a_1(13;z) = 1 + 2z + 2z^2$, $a_1(17;z) = 1 + 4z$, and $a_1(31;z) = 1 + z + z^2 + z^3 + z^4$ are all irreducible.

3. Auxiliary Polynomials and a Theorem of Fuchs

In preparation for some results in the next section we define, for integers $t \geq 2$ and $k \geq 1$,

$$P_k^{(t)}(z) := z + z^t + z^{t^2} + \cdots + z^{t^{k-1}}. \tag{3.1}$$

These polynomials are closely related to the polynomials $a_t(2^k - 1; z)$, as we shall see later. The purpose of this section is to apply a useful and interesting result of

Fuchs [10], given in more modern language by Evans [8] and quoted here in different notation. We follow the development in [4], which dealt with the special case $t = 2$.

We fix an integer $t \geq 2$, and for an integer $n \geq 2$ with $\gcd(n, t) = 1$ we let $\gamma_t(n)$ be the order of t modulo n, i.e., $\gamma_t(n)$ is the smallest positive exponent γ for which $t^\gamma \equiv 1 \pmod{n}$.

Proposition 3.1. *Let $t \geq 2$ be an integer. Then for $n \geq 2$, $\gcd(n, t) = 1$, we have that*

$$\Phi_n(z) \,\Big|\, P^{(t)}_{\gamma_t(n)}(z) \quad \text{if and only if} \quad \gamma_t(n) = p\gamma_t(\tfrac{n}{p}) \quad \text{for some } p \mid n. \tag{3.2}$$

This result is supplemented by the following lemma. In the case $t = 2$ this reduces to Lemma 2.1 in [4], with the proof being very similar.

Lemma 3.1. *Let $t \geq 2$ be an integer. Then for any $n \geq 1$,*

$$\text{if} \quad \Phi_n(z) \,\Big|\, P^{(t)}_k(z) \quad \text{then} \quad \Phi_n(z) \,\Big|\, P^{(t)}_{k\ell}(z) \quad \text{for all integers } \ell \geq 1. \tag{3.3}$$

Proof. We use (3.1) and rearrange the sum as

$$\begin{aligned} P^{(t)}_{k\ell}(z) &= \sum_{j=0}^{\ell-1} \left(z^{t^{jk}} + z^{t^{jk+1}} + z^{t^{jk+2}} + \cdots + z^{t^{jk+k-1}} \right) \\ &= \sum_{j=0}^{\ell-1} \left(\left(z^{t^{jk}} \right)^{t^0} + \left(z^{t^{jk}} \right)^{t^1} + \left(z^{t^{jk}} \right)^{t^2} + \cdots + \left(z^{t^{jk}} \right)^{t^{k-1}} \right). \end{aligned}$$

Now if ζ_n is a primitive nth root of unity then, since we know that n and t are relatively prime, $\zeta_n^{t^{jk}}$ is also a primitive nth root of unity. Therefore, when $z = \zeta_n$, by the hypothesis in (3.3) each of the ℓ summands in the last summation vanishes, and so does $P^{(t)}_{k\ell}(\zeta_n)$; this proves the lemma. $\square$

We will now show that the condition in (3.2), namely

$$\gamma_t(n) = p\gamma_t(\tfrac{n}{p}) \quad \text{for} \quad p \mid n,\ p \nmid t, \tag{3.4}$$

puts further restrictions on n and on $\gamma_t(n)$.

Lemma 3.2. *Let $t \geq 2$ be a fixed integer. If there is a prime $p \nmid t$ and an integer $n \geq 1$ such that (3.4) holds, then*

(a) $p^2 \mid n$;

(b) $p\gamma_t(p) \mid \gamma_t(n)$;

(c) $n \mid p(t^{\gamma_t(p)m} - 1)$ *for some integer $m \geq 1$;*

(d) $p^{u(p)+1} \mid n$*, where* $u(p)$ *is the highest power of* p *dividing* $t^{\gamma_t(p)m} - 1$*.*

Proof. (a) We are going to use the fact that for relatively prime positive integers a, b with $\gcd(a, b) = 1$ we have

$$\gamma_t(ab) = \gamma_t(a)\gamma_t(b). \tag{3.5}$$

Indeed, if we raise the congruences

$$t^{\gamma_t(a)} \equiv 1 \pmod{a}, \qquad t^{\gamma_t(b)} \equiv 1 \pmod{b}$$

to the powers $\gamma_t(b)$ and $\gamma_t(a)$, respectively, then by the Chinese Remainder Theorem we have

$$t^{\gamma_t(a)\gamma_t(b)} \equiv 1 \pmod{ab}.$$

By the minimality of the order we immediately get (3.5).

Now suppose that $p \mid n$ but $p^2 \nmid n$; then clearly $\gcd(p, n/p) = 1$. By (3.5) we then have

$$\gamma_t(n) = \gamma_t(p\tfrac{n}{p}) \leq \gamma_t(p)\gamma_t(\tfrac{n}{p}),$$

and since $\gamma_t(p) \leq p - 1$, this contradicts (3.4), and our assumption $p^2 \nmid n$ was false.

(b) By part (a) we can write

$$\frac{n}{p} = p^{\nu}n', \quad \text{where} \quad \nu \geq 1,\ p \nmid n'.$$

By definition of $\gamma_t(\frac{n}{p})$ we have

$$t^{\gamma_t(n/p)} \equiv 1 \pmod{p^{\nu}n'} \tag{3.6}$$

and therefore, in particular,

$$t^{\gamma_t(n/p)} \equiv 1 \pmod{p}.$$

By the minimality of the order $\gamma_t(p)$ this means that $\gamma_t(p) \mid \gamma_t(n/p)$, and thus $p\gamma_t(n/p)$ is a multiple of $p\gamma_t(p)$. This, with (3.4), proves part (b).

(c) We use (3.6) again, which shows that $\frac{n}{p}$ divides

$$t^{\gamma_t(n/p)} - 1 = t^{\gamma_t(n)/p} - 1 = t^{\gamma_t(p)m} - 1$$

for some $m \geq 1$, by part (b). This proves part (c).

(d) The exponent ν in (3.6) is the same as $u(p)$ in the statement of the result since $\gamma_t(n/p) = \gamma_t(p)m$. The result then follows again from (3.6). $\square$

We now use this lemma to obtain a divisibility result that is more explicit than Proposition 3.1.

Proposition 3.2. *Let $t \geq 2$ be an integer and $p \nmid t$ a prime. Then for all $m \geq 1$ we have that*

$$\Phi_p\left(z^{t^{\gamma_t(p)m}-1}\right) \quad \textit{divides} \quad P^{(t)}_{\gamma_t(p)pm}(z). \tag{3.7}$$

Proof. From (3.1) we get, setting $\gamma := \gamma_t(p)$ for simplicity:

$$\begin{aligned} P_{\gamma pm}(z) = \sum_{j=0}^{\gamma pm-1} z^{t^j} &= \sum_{j=0}^{\gamma m-1}\left(z^{t^j}+z^{t^{\gamma m+j}}+z^{t^{2\gamma m+j}}+\cdots+z^{t^{(p-1)\gamma m+j}}\right) \\ &= \sum_{j=0}^{\gamma m-1} z^{t^j}\left(1+z^{t^j(t^{\gamma m}-1)}+z^{t^j(t^{2\gamma m}-1)}+\cdots+z^{t^j(t^{(p-1)\gamma m}-1)}\right). \end{aligned} \tag{3.8}$$

We now use the fact that

$$\Phi_p(z^{t^{\gamma m}-1})\left(z^{t^{\gamma m}-1}-1\right) = z^{p(t^{\gamma m}-1)}-1, \tag{3.9}$$

which follows from the basic identity $\Phi_p(z) = (z^p-1)/(z-1)$. Our goal is to show that each of the γm terms in large parentheses on the rightmost side of (3.8) is divisible by the leftmost term of (3.9); this would prove (3.7). To do so, we reduce each term on the right of (3.8) modulo the polynomial on the right of (3.9). This can be achieved by reducing the exponents modulo $p(t^{\gamma m}-1)$; that is, we consider, for $\nu = 1, 2, \ldots, p-1$,

$$t^j(t^{\nu\gamma m}-1) = t^j(t^{\gamma m}-1)(t^{(\nu-1)\gamma m}+t^{(\nu-2)\gamma m}+\cdots+t^{\gamma m}+1) \pmod{p(t^{\gamma m}-1)}.$$

Dividing everything by $t^{\gamma m}-1$, the right-hand side becomes

$$t^j(t^{(\nu-1)\gamma m}+t^{(\nu-2)\gamma m}+\cdots+t^{\gamma m}+1) \equiv t^j\nu \pmod{p}$$

since, by definition of γ, we have $t^\gamma \equiv 1 \pmod{p}$. Now, given any integer j, the term $t^j\nu$ runs through a reduced residue system modulo p as ν does. Hence

$$1+z^{t^j(t^{\gamma m}-1)}+z^{t^j(t^{2\gamma m}-1)}+\cdots+z^{t^j(t^{(p-1)\gamma m}-1)} \pmod{z^{p(t^{\gamma m}-1)}-1}$$

is the same for any j, with the terms (other than the initial "1") permuted. We therefore may as well assume that $j = 0$, and we will show that

$$\begin{aligned} &1+z^{t^{\gamma m}-1}+z^{t^{2\gamma m}-1}+\cdots+z^{t^{(p-1)\gamma m}-1} \equiv \Phi_p(z^{t^{\gamma m}-1}) \\ &\quad = 1+z^{t^{\gamma m}-1}+z^{2(t^{\gamma m}-1)}+\cdots+z^{(p-1)(t^{\gamma m}-1)} \pmod{z^{p(t^{\gamma m}-1)}-1}. \end{aligned}$$

To do this, we show that for $\nu = 1, 2, \ldots, p-1$ the corresponding exponents satisfy

$$t^{\nu\gamma m}-1 \equiv \nu(t^{\gamma m}-1) \pmod{p(t^{\gamma m}-1)}. \tag{3.10}$$

Factoring the left-hand side, as we did before, and rearranging, we see that (3.10) is equivalent to

$$(t^{\gamma m}-1)\left[t^{(\nu-1)\gamma m}+t^{(\nu-2)\gamma m}+\cdots+t^{\gamma m}+1-\nu\right]\equiv 0 \pmod{p(2^{tm}-1)}.$$

This is true since the expression in square brackets vanishes modulo p. The proof is now complete. $\square$

To illustrate Proposition 3.2, we state the smallest cases, $p=2$ and $p=3$, as corollaries. First, we note that $\Phi_2(z)=z+1$ and $\gamma_t(2)=1$ for all odd t.

Corollary 3.1. *For all $m\geq 1$ and odd $t\geq 3$ we have*

$$z^{t^m-1}+1\,\Big|\,P_{2m}^{(t)}(z).$$

Next, we use the facts that $\Phi_3(z)=z^2+z+1$ and $\gamma_t(3)=1$ or 2, according as $t\equiv 1$ or $2 \pmod 3$. Proposition 3.2 then gives the following result.

Corollary 3.2. *Let $t\geq 2$ with $3\nmid t$. Then*

$$z^{2(t^m-1)}+z^{t^m-1}+1\,\Big|\,P_{3m}^{(t)}(z)$$

holds for all $m\geq 1$ when $t\equiv 1 \pmod 3$, and for all even $m\geq 2$ when $t\equiv 2 \pmod 3$.

4. The Polynomials $a_t(2^k\pm 1;z)$

In this section we deal with two special infinite classes of generalized Stern polynomials, each with increasing numbers of terms. Using simple inductions based on the identity (1.3), it is easy to see that

$$a_t(2^k+1;z)=1+z+z^t+z^{t^2}+\cdots+z^{t^{k-1}}, \tag{4.1}$$

$$a_t(2^k-1;z)=1+z+z^{t+1}+z^{t^2+t+1}+\cdots+z^{t^{k-2}+t^{k-3}+\cdots+t+1}. \tag{4.2}$$

4.1. The Polynomials $a_t(2^k+1;z)$

In [3] we proved a result on the reducibility and factors of $a_t(2^k+1;z)$ for $t=2$. Here we are going to extend this result to arbitrary integers $t\geq 2$.

Proposition 4.1. *Let $t\geq 2$ be an integer, and let $p\geq 3$ be a prime which has t as a primitive root. Then*

$$(1+z+z^2+\cdots+z^{p-1})\,\big|\,a_t(2^{p-1}+1;z).$$

In particular, $a_t(2^{p-1}+1;z)$ is reducible in this case, with the exception of $a_2(5;z)=1+z+z^2$.

Proof. If t is a primitive root of p, then $t^0, t^1, \ldots, t^{p-2}$ is a reordering of $1, 2, \ldots, p-1 \pmod{p}$. Therefore with (4.1) we have

$$a_t(2^{p-1}+1; z) = 1 + \sum_{j=0}^{p-2} z^{t^j} \equiv 1 + \sum_{j=1}^{p-1} z^j \pmod{z^p - 1}.$$

Since $(z^{p-1} + \cdots + z + 1)(z-1) = z^p - 1$, this shows that $a(2^{p-1}+1; z)$ is divisible by $z^{p-1} + \cdots + z + 1$. When $t = 2$ and $p = 3$, we see that $a_2(5; z) = 1 + z + z^2$ is its own irreducible factor. □

When $p = 5$, it is easy to verify that $t = 2$ and $t = 3$ are primitive roots modulo 5, and so are all other positive integers $t \equiv 2, 3 \pmod{p}$. Hence Proposition 2.6(a) follows immediately from Proposition 3.1.

The next smallest case is $p = 7$, and its primitive roots are $t = 3$ and $t = 5$. Thus we get the following analogue of Proposition 2.6(a).

Corollary 4.1. *If $t \equiv 3, 5 \pmod{7}$, then $\Phi_7(z)$ divides $a_t(65; z)$.*

Obviously, for any odd prime p we could write down such a statement, where according to the theory of primitive roots there are $\varphi(p-1)$ relevant residue classes of $t \pmod{p}$.

4.2. The Polynomials $a_t(2^k - 1; z)$

We begin by proving an easy analogue of Proposition 3.1.

Proposition 4.2. *Let $p \geq 3$ be a prime and $t \geq 2$ be an integer satisfying $t \equiv 1 \pmod{p}$. Then*

$$(1 + z + z^2 + \cdots + z^{p-1}) \,|\, a_t(2^p - 1; z).$$

In particular, $a_t(2^p - 1; z)$ is reducible in this case.

Proof. When $t \equiv 1 \pmod{p}$, then for $j \geq 1$ we have $t^{j-1} + \cdots + t + 1 \equiv j \pmod{p}$, and so by (4.2),

$$a_t(2^p - 1; z) \equiv 1 + z + z^2 + \cdots + z^{p-1} \pmod{z^p - 1}.$$

The conclusion now follows as in the proof of Proposition 3.1. □

It is clear that Proposition 2.6(b) is a special case of this result.

In preparation for the next results we use $t^{j-1} + \cdots + t + 1 = (t^j - 1)/(t-1)$ (for $j \geq 1$) to rewrite the identity (4.2) as

$$z a_t(2^k - 1; z^{t-1}) = z + z^t + z^{t^2} + \cdots + z^{t^{k-1}}, \tag{4.3}$$

and by (3.1) we have

$$P_k^{(t)}(z) = z a_t(2^k - 1; z^{t-1}). \tag{4.4}$$

In order to apply Proposition 3.2, we use the notation

$$[j]_t := \frac{t^j - 1}{t - 1} = t^{j-1} + \cdots + t + 1.$$

Then, by replacing z^{t-1} by z, we immediately get the following result from Proposition 3.2 and from (4.4).

Proposition 4.3. *Let $t \geq 2$ be an integer and $p \nmid t$ a prime. Then for all $m \geq 1$ we have*

$$\Phi_p(z^{[\gamma_t(p)m]_t}) \Big| a_t(2^{\gamma_t(p)pm} - 1; z)\ . \tag{4.5}$$

The polynomial on the right of (4.5) is reducible, with the exception of the case $m = 1$, $p = 2$, and odd $t \geq 3$.

Before proving this, we state some special cases. First, when $t \equiv 1 \pmod{p}$, then $\gamma_t(p) = 1$, and we get the following consequence of (4.5).

Corollary 4.2. *Let p be a prime and $t \geq 2$ an integer with $t \equiv 1 \pmod{p}$. Then for all $m \geq 1$ we have*

$$\Phi_p(z^{[m]_t})\, | a_t(2^{pm} - 1; z)\ . \tag{4.6}$$

The polynomial on the right of (4.6) is reducible, with the exception of the case $m = 1$, $p = 2$, and odd $t \geq 3$, in which case $a_t(3; z) = 1 + z$ is its own cyclotomic factor.

Proof. Only the statement concerning reducibility remains to be shown. The factor on the left of (4.6) has p terms, while the polynomial $a_t(2^{pm} - 1; z)$ has pm terms (see (4.2)); this forces $m = 1$. Next, the degree of $\Phi_p(z^{[1]_t}) = \Phi_p(z)$ is $p - 1$, while that of $a_t(2^p - 1; z)$ is $1 + t + \cdots + t^{p-2}$, again by (4.2). Since $t > 1$, this forces p to be 2, which proves the assertion. $\square$

We note that the case $m = 1$ and $p \geq 3$ reduces to Proposition 4.2, thus giving a different proof of that result.

Proof of Proposition 4.3. Once again, only the reducibility assertion remains to be shown. With a similar argument as in the previous proof, we note that the cyclotomic factor on the left of (4.5) has p terms, while the Stern polynomial on the right of (4.5) has $\gamma_t(p)pm$ terms. This forces $m = 1$ and $\gamma_t(p) = 1$, which is a special case of Corollary 4.2. The assertion now follows from the proof of Corollary 4.2. $\square$

In analogy to Corollaries 3.1 and 3.2 we immediately get the following special cases.

Corollary 4.3. *For all $m \geq 1$ and odd $t \geq 3$ we have*

$$z^{[m]_t} + 1 \,\big|\, a_t(2^{2m} - 1; z) \, .$$

As a consequence, the polynomial $a_t(2^{2m} - 1; z)$ is reducible, with the exception of the case $m = 1$.

Corollary 4.4. *Let $t \geq 2$ with $3 \nmid t$. Then*

$$z^{2[m]_t} + z^{[m]_t} + 1 \,\big|\, a_t(2^{3m} - 1; z)$$

holds for all $m \geq 1$ when $t \equiv 1 \pmod 3$, and for all even $m \geq 2$ when $t \equiv 2 \pmod 3$. The polynomial $a_t(2^{3m} - 1; z)$ is reducible.

Example 1. Let $t = 5$; then we can use Corollary 4.3 with $m = 3$ and Corollary 4.4 with $m = 2$ to find factors of $a_5(2^6 - 1; z)$. We compute

$$\begin{aligned} z^{[3]_5} + 1 &= z^{31} + 1 = (z+1)(z^{30} - z^{29} + z^{28} - \cdots - z + 1) = \Phi_2(z)\Phi_{62}(z), \\ z^{2[2]_5} + z^{[2]_5} + 1 &= z^{12} + z^6 + 1 = (z^6 + z^3 + 1)(z^6 - z^3 + 1) = \Phi_9(z)\Phi_{18}(z). \end{aligned}$$

By (4.2), the polynomial $a_5(2^6 - 1; z)$ has degree $5^4 + 5^3 + 5^2 + 5 + 1 = 781$ (see also [5] for a general formula for the degree of $a_t(n; z)$). A computation shows that the four factors above are the only cyclotomic factors; the 738-degree noncyclotomic part is irreducible and has no zeros of modulus 1.

Example 2. To find cyclotomic factors of $a_4(2^{30} - 1; z)$, we can once again use Corollary 4.4, while Corollary 4.3 does not apply. However, Proposition 4.3 can be used with $p = 5$, if we note that $\gamma_4(5) = 2$ since $4^2 \equiv 1 \pmod 5$. Then (4.5) with $m = 3$ shows that

$$\Phi_5(z^{1365}) \mid a_4(2^{30} - 1; z)$$

since $[6]_4 = (4^6 - 1)/3 = 1365$. Now, since

$$\Phi_5(z^{1365})(z^{1365} - 1) = z^{5 \cdot 1365} - 1, \tag{4.7}$$

we can apply the fundamental identity

$$z^n - 1 = \prod_{d|n} \Phi_d(z) \tag{4.8}$$

(twice) to find that

$$\Phi_5(z^{1365}) = \prod_{d \in A} \Phi_d(z),$$

where $A := \{25, 75, 175, 325, 525, 975, 2275, 6825\}$.

Next, Corollary 4.4 with $m = 10$ (which is actually a special case of Proposition 4.3 with $p = 3$) shows that

$$z^{2[10]_4} + z^{[10]_4} + 1 \mid a_4(2^{30} - 1; z),$$

and with $[10]_4 = 349\,525$ and using analogues to (4.7) and (4.8), we find that

$$z^{2[10]_4} + z^{[10]_4} + 1 = \prod_{d\in B} \Phi_d(z),$$

where $B := \{3, 15, 33, 75, 93, 123, 165, 465, 615, 825, 1\,023, 1\,353, 2\,325, 3\,075, 3\,813, 5\,115, 6\,765, 19\,065, 25\,575, 33\,825, 41\,943, 95\,325, 209\,715, 1\,048\,575\}$. The polynomial $a_4(2^{30}-1; z)$, which has degree $\frac{1}{3}(4^{29}-1)$, is therefore divisible by all cyclotomic polynomials $\Phi_d(z)$ with $d \in A \cup B$.

5. Derivatives and Multiple Factors

We note that in Example 2 above the subscript $d = 75$ occurs in both sets A and B. Does this mean that $a_4(2^{30}-1; z)$ is divisible by $\Phi_{75}(z)^2$? In [4] we showed that no polynomial $a_2(2^k-1; z)$ is divisible by the square of a cyclotomic polynomial. We will use the same method as in [4] to prove the following extension of this result.

Proposition 5.1. *No polynomial $a_t(2^k \pm 1; z)$, $t \ge 2$ and $k \ge 1$, is divisible by the square of a cyclotomic polynomial.*

The main ingredient in the proof is the following result on the distribution of zeros (in this case critical points) of polynomials.

Proposition 5.2. *All the critical points of the polynomials $a_t(2^k \pm 1; z)$, $t \ge 2$ and $k \ge 1$, lie in the interior of the unit circle.*

Proof. By (4.1) we have

$$\frac{d}{dz} a_t(2^k+1; z) = 1 + tz^{t-1} + t^2 z^{t^2-1} + \cdots + t^{k-2} z^{t^{k-2}-1} + t^{k-1} z^{t^{k-1}-1}.$$

Now set

$$Q(z) := t^{k-1} z^{t^{k-1}-1}, \qquad P(z) := \frac{d}{dz} a_t(2^k+1; z) - Q(z).$$

Then for $|z| = 1$ we have $|Q(z)| = t^{k-1}$, while

$$|P(z)| \le 1 + t + t^2 + \cdots + t^{k-2} = \frac{t^{k-1}-1}{t-1} < |Q(z)|,$$

where the last inequality holds for $t \ge 2$. Hence by Rouché's theorem (see, e.g., [15, p. 2]), the polynomial $P(z) + Q(z) (= \frac{d}{dz} a_t(2^k+1; z))$ has the same number of zeros inside the unit circle as does $Q(z)$, namely $t^{k-1}-1$, which is all of them. This completes the proof for $a_t(2^k+1; z)$.

Next, by (4.3) we have

$$a_t(2^k-1; z^{t-1}) = 1 + z^{t-1} + z^{t^2-1} + \cdots + z^{t^{k-2}-1} + z^{t^{k-1}-1},$$

and the same method as used above for $a_t(2^k+1;z)$ shows that the critical points of $a_t(2^k-1;z^{t-1})$ lie inside the unit circle. As a consequence, the polynomial $a_t(2^k-1;z)$ has the same property. Indeed, if a critical point of $a_t(2^k-1;z)$ were to lie on or outside the unit circle, then by the chain rule this would also be the case for $a_t(2^k-1;z^{t-1})$, a contradiction. The proof is now complete. □

Proof of Proposition 5.1. We assume that some $\Phi_d(z)^2$ divides a certain $a_t(2^k \pm 1;z)$. But then the zeros of $\Phi_d(z)$, which by definition are roots of unity, would be critical points of $a_t(2^k \pm 1;z)$, which contradicts Proposition 5.2. □

In [4] we proved that $P_{k+1}^{(2)}(z)$, in the present paper defined by (3.1), has an irreducible derivative whenever k is a power of a prime. We will now see that this result can be considerably extended.

Proposition 5.3. *Let $t = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $r \geq 1$, where $p_1, \dots p_r$ are distinct primes and $\alpha_j \geq 1$ for $1 \leq j \leq r$. If $\alpha_j \mid t$ for at least one j, $1 \leq j \leq r$, then $\frac{d}{dz}a_t(2^{k+1}+1;z)$ and $\frac{d}{dz}P_{k+1}^{(t)}(z)$ are irreducible whenever $k = q^\beta$ for some prime $q \nmid t-1$ and $\beta \geq 1$.*

Proof. By (4.1) and (4.4) with (4.3), the polynomials $a_t(2^{k+1}+1;z)$ and $P_{k+1}^{(t)}(z)$ have the same derivative

$$F(z) := 1 + tz^{t-1} + t^2 z^{t^2-1} + \cdots + t^k z^{t^k-1}. \tag{5.1}$$

We now use the method of Newton polygons (see, e.g., [17, p. 55]), as we did in [4] for $t = 2$. Let j be such that $\alpha_j \mid t$, and for simplicity of notation we set $\alpha := \alpha_j$, $p := p_j$. With this prime p as base, the points of the polynomial $F(z)$ are, by (5.1),

$$(0,0),\ (t-1,\alpha),\ (t^2-1,2\alpha),\ (t^3-1,3\alpha), \dots,\ (2^k-1,k\alpha).$$

Here (a,b) is a point in this sequence if the coefficient of z^a of the polynomial $F(z)$ is exactly divisible by p^b. Zero coefficients are not listed as points.

Since $j\alpha/(t^j-1)$ is a strictly decreasing sequence for $j \geq 1$, all the points for $1 \leq j \leq k-1$ lie strictly above the line segment connecting $(0,0)$ with $(t^k-1,k\alpha)$. Therefore the Newton polygon for $F(z)$ with prime p is just this line segment, as required by the irreducibility criterion. Another condition is that $\gcd(t^k-1,k\alpha) = 1$. Since by hypothesis $\alpha \mid t$, this reduces to $\gcd(t^k-1,k) = 1$. Let $k = q^\beta$ for a prime q; then by Fermat's little theorem we have $t^q \equiv t \pmod{q}$, and upon iterating,

$$t^{q^\beta} \equiv t \pmod{q}, \quad \text{or} \quad t^k - 1 \equiv t - 1 \pmod{q}.$$

Therefore, if $q \nmid t-1$, then $\gcd(t^k-1,k) = 1$, and the proof of the irreducibility of $F(z)$ is complete. □

As an immediate consequence of Proposition 5.3, we get the following result, which supplements Proposition 5.1 as it addresses the question of multiple factors that are not cyclotomic polynomials.

Proposition 5.4. *Let $t = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $r \geq 1$, where $p_1, \dots p_r$ are distinct primes and $\alpha_j \geq 1$ for $1 \leq j \leq r$. If $\alpha_j \mid t$ for at least one j, $1 \leq j \leq r$, then $a_t(2^{k+1}+1; z)$ and $a_t(2^{k+1}-1; z)$ have no multiple roots whenever $k = q^\beta$ for some prime $q \nmid t-1$ and $\beta \geq 1$.*

Proof. If $a_t(2^{k+1}+1; z)$ had a multiple root, then this polynomial and its derivative would have this root in common. However, since by Proposition 5.3 the derivative is irreducible, it would be a divisor of $a_t(2^{k+1}+1; z)$. This is impossible, as can be seen by comparing (2.1) with (4.1).

Similarly, we see that $P_{k+1}^{(t)}(z)$ has no multiple roots under the given conditions. As a consquence of this and (4.4), the polynomial $a_t(2^{k+1}-1; z)$ also has no multiple root. □

Clearly, most integers t satisfy the condition "$\alpha_j \mid t$ for at least one j" in Propositions 5.3 and 5.4. In fact, a quick calculation shows that only 24 values of $t \leq 1000$ do not, those up to 100 being $t = 8$, 9, 25, 32, 49, 64, and 81. In particular, these exceptions include all squares of odd integers.

6. Further Remarks

Since this paper deals with Stern polynomials, it should be mentioned that a polynomial extension of the Stern sequence, different from that in [6], was independently introduced by Klavžar et al. [11]. Interestingly, their sequence of polynomials, which are not $(0, 1)$-polynomials, is also related to hyperbinary expansions of n.

Combining results from Sections 2 and 4 with further computations, we observe that the only subscripts $n < 100$ for which $a_t(n; z)$ is reducible for some $t \leq 19$ are 3, 5, 7, 15, 17, 27, 31, 35, 45, 51, 55, 63, 65, 75, 85, and 99; there is a total of 82 such odd subscripts $n < 1000$.

References

[1] B. Bates and T. Mansour, *The q-Calkin-Wilf tree*, J. Combin. Theory Ser. A **118** (2011), 1143–1151.

[2] N. Calkin and H. S. Wilf, *Recounting the rationals*, Amer. Math. Monthly **107** (2000), no. 4, 360–363.

[3] K. Dilcher and L. Ericksen, *Reducibility and irreducibility of Stern* $(0, 1)$*-polynomials*, Commun. Math. **22** (2014), 77–102.

[4] K. Dilcher and L. Ericksen, *The polynomials of Mahler and roots of unity*, Amer. Math. Monthly **122** (2015), no. 4, 338–353.

[5] K. Dilcher and L. Ericksen, *Hyperbinary expansions and Stern polynomials*, Electron. J. Combin. **22** (2015), no. 2, Article P2.24, 18 pp.

[6] K. Dilcher and K. B. Stolarsky, *A polynomial analogue to the Stern sequence*, Int. J. Number Theory **3** (2007), no. 1, 85–103.

[7] K. Dilcher and K. B. Stolarsky, *Stern polynomials and double-limit continued fractions*, Acta Arith. **140** (2009), no. 2, 119–134.

[8] R. J. Evans, *Generalized cyclotomic periods*, Proc. Amer. Math. Soc. **81** (1981), 207–212.

[9] C. Finch and L. Jones, *On the irreducibility of* $\{-1, 0, 1\}$*-quadrinomials*, Integers **6** (2006), A16, 4 pp.

[10] L. Fuchs, *Ueber die Perioden, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn* n *eine zusammengesetzte Zahl ist*, J. Reine Angew. Math. **61** (1863), 374–386.

[11] S. Klavžar, U. Milutinović, and C. Petr, *Stern polynomials*, Adv. in Appl. Math. **39** (2007), 86–95.

[12] D. H. Lehmer, *On Stern's diatomic series*, Amer. Math. Monthly **36** (1929), 59–67.

[13] T. Mansour, *q-Stern polynomials as numerators of continued fractions*, Bull. Polish Acad. Sci. Math. **63** (2015), no. 1, 11–18.

[14] T. Mansour and M. Shattuck, *Two further generalizations of the Calkin–Wilf tree*, J. Comb. **2** (2011), no. 4, 507–524.

[15] M. Marden, *Geometry of Polynomials*, American Mathematical Society, Providence, RI, 1966.

[16] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

[17] V. V. Prasolov, *Polynomials*, Springer-Verlag, Berlin, 2004.

[18] B. Reznick, *Some binary partition functions*, in Analytic Number Theory, Proceedings of a conference in honor of Paul T. Bateman, B. C. Berndt et al., eds. (Birkhäuser, Boston, 1990), pp. 451–477.

[19] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.

[20] R. P. Stanley and H. S. Wilf, *Refining the Stern diatomic sequence*, preprint, 2010, `http://www-math.mit.edu/~rstan/papers/stern.pdf`.

[21] M. A. Stern, *Ueber eine zahlentheoretische Funktion*, J. Reine Angew. Math. **55** (1858), 193–220.

[22] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$, Math. Scand. **8** (1960), 121–126.