

FEKETE-LIKE POLYNOMIALS

KEVIN G. HARE AND SOROOSH YAZDANI

Dedicated to Peter Borwein on the occasion of his 55th birthday.

ABSTRACT. In 2001, Borwein, Choi, and Yazdani looked at an extremal property of a class of polynomial with ± 1 coefficients. Their key result was:

Theorem (Borwein, Choi, Yazdani, 2001). *Let $f(z) = \pm z \pm z^2 \pm \dots \pm z^{N-1}$, and ζ a primitive N th root of unity. If N is an odd positive integer then*

$$\max_i |f(\zeta^i)| \geq \sqrt{N}$$

with equality if and only if N is an odd prime.

Moreover, if equality holds, they gave an explicit construction for $f(z)$. In this paper, we look at the case when N is even. In particular, we investigate the following

Conjecture. *Let $f(z)$ and ζ be as above. If $N > 2$ is an even positive integer then*

$$\max_i |f(\zeta^i)| \geq \sqrt{N+1}$$

with equality if and only if $N+1$ is a power of an odd prime.

This conjecture was made after extensive computations. Partial results towards proving this conjecture are given.

1. INTRODUCTION

The goal of this paper is to study the following

Conjecture 1.1. *Let $f(z) = \pm z \pm z^2 \pm \dots \pm z^{N-1}$. Let ζ be a primitive N th root of unity. If $N > 2$ is an even positive integer then*

$$(1.1) \quad \max_i |f(\zeta^i)| \geq \sqrt{N+1}$$

with equality if and only if $N+1$ is a power of an odd prime.

For ease of notation, let

$$\mathcal{L}_N = \{ \pm z \pm z^2 \pm \dots \pm z^{N-1} \}$$

be the set of Littlewood-like polynomials of degree $N-1$. For $f = \sum_{i=1}^{N-1} a_i z^i \in \mathcal{L}_N$, let $f^* = \sum_{i=1}^{N-1} a_{N-i} z^i$ be the reciprocal polynomial (i.e. $f^*(z) = z^N f(1/z)$), and

$$\mathcal{A}_N = \left\{ f(z) \in \mathcal{L}_N \mid f(z) = (-1)^{N/2} f^*(-z) \right\}$$

Date: October 17, 2008.

2000 Mathematics Subject Classification. Primary: 11J54, 11B83, 12-04.

Research of K. G. Hare supported, in part by NSERC of Canada.

Research of S. Yazdani supported, in part by NSERC of Canada .

The authors would like to thank IRMACS (SFU) for their hospitality and support.

be the subset of anti-skewsymmetric polynomials. We let $a_0 = 0$ throughout this paper. Note that if $f(z) = \sum_i a_i z^i \in \mathcal{A}_N$ then $a_{N-i} = (-1)^{N/2+i} a_i$. We say that a polynomial $f \in \mathcal{L}_N$ or \mathcal{A}_N that satisfies equation (1.1) with equality is an *optimal polynomial*.

Conjecture 1.1 was made after extensive computation in the space of Littlewood-like polynomials. Specifically this conjecture is verified for $N \leq 42$ for all Littlewood-like polynomials, and for $N \leq 84$ for anti-skewsymmetric polynomials. More on these, and other computations can be found in Section 5.

In [5], the case when N is odd was investigated:

Theorem 1.2 (Borwein, Choi, Yazdani, 2001). *Let $f(z) = \sum_{i=1}^{N-1} a_i z^i \in \mathcal{L}_N$ and ζ a primitive N th root of unity. If N is an odd positive integer then*

$$\max_i |f(\zeta^i)| \geq \sqrt{N}$$

with equality if and only if N is prime. Moreover, if equality holds, then $a_1 f(z)$ is the Fekete polynomial, that is $a_i = a_1 \left(\frac{i}{N}\right)$, where $\left(\frac{i}{N}\right)$ is the Legendre symbol.

Notice, if N is a prime number, and f is the Fekete polynomial of degree $N-1$, then for ζ a primitive N th root of unity we have that $|f(\zeta^i)| = \sqrt{N}$ for $i = 1, 2, \dots, N-1$ and $f(1) = 0$.

Throughout this paper, let p be an odd prime and $q = p^k$ a prime power. Let \mathbb{F}_q be the finite field with q elements in it. We denote \mathbb{F}_q^* the group of invertible elements in \mathbb{F}_q . Let $\chi : \mathbb{F}_q \rightarrow \{0, \pm 1\}$ be the quadratic residue map, that is $\chi(c) + 1$ is the number of solutions to $z^2 = c$ in \mathbb{F}_q . It is well known that χ restricted to \mathbb{F}_q^* is a group map to the group of two elements. If $N+1 = q = p^k$, then \mathbb{F}_q will have a primitive N th root of unity, which we will denote by r .

Note that $\mathcal{L}_N \subset \mathbb{Z}[x]$, however in some cases it is useful to treat $\mathcal{L}_N \subset \mathbb{F}_q[x]$. When $N+1 = q$, for any choice of ζ and r a primitive N th root of unity, there is a natural map π taking $\mathbb{Z}[\zeta]$ to \mathbb{F}_q , sending ζ to r .

In Section 2 for N even, we show that:

Theorem 1.3. *Let $f \in \mathcal{A}_N$, and ζ a primitive N th root of unity. If $N > 2$ is an even number then*

$$(1.2) \quad \max_i |f(\zeta^i)| \geq \sqrt{N+1}.$$

Furthermore, if equality is achieved then $|f(\zeta^i)| = \sqrt{N+1}$ for all but two values of $i \in \{0, 1, \dots, N-1\}$. At these other two values of i , we have $|f(\zeta^i)| = 1$.

In the above theorem, we needed the assumption that $f \in \mathcal{A}_N$ in the proof. This is somewhat unfortunate, because computationally it appears that for $f \in \mathcal{L}_N$ whenever the inequality 1.2 is satisfied, we have $f \in \mathcal{A}_N$ (see Section 5). If we could replace \mathcal{A}_N in Theorem 1.3 with \mathcal{L}_N , then we would have proved one part of Conjecture 1.1. The proof is similar to the case when N is odd, although we have to work slightly more because the parity argument in [5] fails in this case.

In Section 3, for $N+1$ a prime power, we construct a Littlewood polynomial g satisfying $\max_i |g(\zeta^i)| = \sqrt{N+1}$. Most f found satisfy this property, (see Section 5), but there are a few unusual exceptions to this rule. None of these exceptions contradict Conjecture 1.1, and none of them occur when $N+1$ is not a power of a odd prime.

We will present some evidence for Conjecture 1.1 in Section 4 by proving it under extra (unfortunately fairly restrictive) assumptions on f .

In Section 5 we give some computational evidence in support of our conjecture. In addition, we make some concluding comments, and list some possible future directions for this work.

2. A PROOF OF THEOREM 1.3

The proof of this theorem is similar to the odd N case, although the parity argument needs to be modified. Let $\zeta \in \mathbb{C}$ be a primitive N th root of unity. Let

$$h(z) = \sum_{k=0}^{N-1} c_k z^k$$

where $c_k = \sum_{j-\ell \equiv k} a_j a_\ell$ and the sum is over all $0 \leq j, \ell < N$ with $j - \ell \equiv k \pmod{N}$. (Recall that $a_0 = 0$.) We have the following:

$$\begin{aligned} \sum_{i=0}^{N-1} |f(\zeta^i)|^2 &= \sum_{i=0}^{N-1} f(\zeta^i) f(\zeta^{-i}) \\ &= \sum_{i=0}^{N-1} \sum_{l=1}^{N-1} \sum_{j=1}^{N-1} a_j a_l \zeta^{i(j-l)} \\ &= \sum_{i=0}^{N-1} \sum_{k=0}^{N-1} \sum_{j-l \equiv k} a_j a_l \zeta^{ki} \\ &= \sum_{i=0}^{N-1} h(\zeta^i) \\ &= Nc_0 \\ &= N(N-1). \end{aligned}$$

Looking at the 4-norm gives us:

$$\begin{aligned}
\sum_{i=0}^{N-1} |f(\zeta^i)|^4 &= \sum_{i=0}^{N-1} (f(\zeta^i)f(\zeta^{-i})) (f(\zeta^{-i})f(\zeta^i)) \\
&= \sum_{i=0}^{N-1} h(\zeta^i)h(\zeta^{-i}) \\
&= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} c_j c_k \zeta^{i(j-k)} \\
&= \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} c_j c_k \sum_{i=0}^{N-1} \zeta^{i(j-k)} \\
&= N \sum_{j=0}^{N-1} c_j^2 \\
&= N(N-1)^2 + N \sum_{j=1}^{N-1} c_j^2.
\end{aligned}$$

Now if $a_j a_\ell \neq 0$ we have $a_j a_\ell \equiv a_j + a_\ell - 1 \pmod{4}$. Furthermore, $a_0 a_k = 0 \equiv a_0 + a_k - 1 + (1 - a_k) \pmod{4}$. Therefore

$$\begin{aligned}
c_k &= \sum_{j-\ell \equiv k} a_j a_\ell \\
&\equiv \left(\sum_{j-\ell \equiv k} a_j + a_\ell - 1 \right) + (1 - a_k) + (1 - a_{N-k}) \pmod{4} \\
&\equiv 2 \left(\sum_j a_j \right) - N + 2 - (a_k + a_{N-k}) \pmod{4} \\
&\equiv 2f(1) + N + 2 - (a_k + a_{N-k}) \pmod{4} \\
&\equiv 2 + N + 2 - (a_k + a_{N-k}) \pmod{4} \\
&\equiv N - (a_k + a_{N-k}) \pmod{4}
\end{aligned}$$

Since we are assuming that $f \in \mathcal{A}_N$, we have that $a_{N-k} = (-1)^{k+N/2} a_k$, we get

$$\begin{aligned}
c_k &\equiv N - a_k(1 + (-1)^{k+N/2}) \pmod{4} \\
&\equiv N + (1 + (-1)^{k+N/2}) \pmod{4} \\
&\equiv \begin{cases} 2 & \text{if } k \text{ even,} \\ 0 & \text{if } k \text{ odd.} \end{cases}
\end{aligned}$$

Therefore $|c_k| \geq 2$ when k is even, and so $c_k^2 \geq 4$. Therefore

$$\begin{aligned} \sum_{i=0}^{N-1} |f(\zeta^i)|^4 &= N(N-1)^2 + N \sum_{k=1}^{N-1} c_k^2 \\ &\geq N(N-1)^2 + N \left(\frac{N-2}{2} \right) 4 = N(N^2 - 3). \end{aligned}$$

This gives us

$$\begin{aligned} \sum_{i=0}^{N-1} |f(\zeta^i)|^2 - 1 &= N(N-2), \\ \sum_{i=0}^{N-1} (|f(\zeta^i)|^2 - 1)^2 &\geq N^2(N-2). \end{aligned}$$

Note that f is assumed anti-skewsymmetric, and hence

$$|f(\zeta^i)| = |f(-\zeta^i)| = |f(\zeta^{i+N/2})|.$$

Therefore we have

$$(2.1) \quad \sum_{i=0}^{N/2-1} |f(\zeta^i)|^2 - 1 = N(N-2)/2,$$

$$(2.2) \quad \sum_{i=0}^{N/2-1} (|f(\zeta^i)|^2 - 1)^2 \geq N^2(N-2)/2.$$

Let $x_i = \frac{N+1-|f(\zeta^i)|^2}{N}$. From (2.1) and (2.2) we get that

$$\begin{aligned} \sum x_i &= 1 \\ \sum x_i^2 &\geq 1 \end{aligned}$$

If $\max_i |f(\zeta^i)| \leq \sqrt{N+1}$ then $0 \leq x_i$, and since $\sum x_i = 1$ we have $x_i \leq 1$. Hence $x_i^2 \leq x_i$, for all i . But this gives that

$$1 \leq \sum x_i^2 \leq \sum x_i = 1$$

which implies that $x_i^2 = x_i$ (hence $x_i \in \{0, 1\}$) for all i . In particular, this implies that $x_i = 0$ for all except exactly one x_i . Translating back to information about $f(\zeta)$ we get

$$\max_i |f(\zeta^i)| \geq \sqrt{N+1}.$$

If equality holds, then $|f(\zeta^i)| = \sqrt{N+1}$ for all but two values of i , where the value at the remaining two values is 1.

By noticing that $f \in \mathcal{A}_N$ we have

$$|f(\zeta^i)| = |f(\zeta^{-i})| = |f(-\zeta^i)| = |f(-\zeta^{-i})|$$

hence we see that if $f(\zeta^i) = \pm 1$, then $\zeta^i = \pm 1$, or $\zeta^i = \pm\sqrt{-1}$.

3. A CONSTRUCTION GIVING EQUALITY

In this section, we will give a constructive proof for a polynomial with the desired property.

Theorem 3.1. *Let $N = q - 1 = p^k - 1$ be one less than a prime power. Let r be a primitive N th root of unity in \mathbb{F}_q . Define*

$$(3.1) \quad g(z) = \sum_{i=1}^{N-1} a_i z^i,$$

with $a_i = \chi(r^i - 1)$ where χ is the quadratic residue map. Then $g(z) \in \mathcal{A}_N$, and has the desired property that

$$\max_i |g(\zeta^i)| = \sqrt{N+1}$$

where ζ is a primitive N th root of unity.

We say that a polynomial $\pm g(z)$ constructed via Theorem 3.1 is a *Fekete-like* polynomial. We first need the following well known

Lemma 3.2. *For any $b \in \mathbb{F}_q$ we have*

$$(3.2) \quad \sum_{a \in \mathbb{F}_q} \chi(a)\chi(a+b) = \begin{cases} -1 & \text{if } b \neq 0, \\ q-1 & \text{if } b = 0. \end{cases}$$

See [7] for discussions on Lemma 3.2, and more general problems relating to it.

Proof of Theorem 3.1. We use Lemma 3.2 to calculate $|g(\zeta^k)|^2$. Note that

$$\begin{aligned} |g(\zeta^k)|^2 &= g(\zeta^k)g(\zeta^{-k}) \\ &= \sum_{\ell, j} \chi(r^\ell - 1)\chi(r^j - 1)\zeta^{k(\ell-j)} \\ &= \sum_{i, j} \chi(r^{i+j} - 1)\chi(r^j - 1)\zeta^{ki} \\ &= \sum_{i, j} \chi(r^i)\chi(r^j - r^{-i})\chi(r^j - 1)\zeta^{ki} \\ &= \sum_{i, j} \chi(r^i)\chi(r^j - 1 - (r^{-i} - 1))\chi(r^j - 1)\zeta^{ki} \\ &= \sum_i (-1)^i \zeta^{ki} \sum_j \chi(r^j - 1)\chi(r^j - 1 - (r^{-i} - 1)). \end{aligned}$$

Let $1 - r^{-i} = b$, then the inner sum becomes

$$\begin{aligned}
\sum_j \chi(r^j - 1)\chi(r^j - 1 + b) &= \left(\sum_{a \in \mathbb{F}_q} \chi(a)\chi(a + b) \right) - \chi(-1)\chi(-1 + b) \\
&= \left(\sum_{a \in \mathbb{F}_q} \chi(a)\chi(a + b) \right) - \chi(1 - (1 - r^{-i})) \\
&= \left(\sum_{a \in \mathbb{F}_q} \chi(a)\chi(a + b) \right) - \chi(r^{-i}) \\
&= \begin{cases} -1 - (-1)^i & \text{if } b \neq 0, \\ q - 2 & \text{if } b = 0. \end{cases}
\end{aligned}$$

Therefore the inner sum is just $-1 - (-1)^i$, and hence

$$\begin{aligned}
|g(\zeta^k)|^2 &= q - 2 + \sum_{i=1}^{q-2} (-1)^i \zeta^{ki} (-1 - (-1)^i) \\
&= q - \sum_{i=0}^{q-2} (\zeta^{ki} + (-\zeta)^{ki}) \\
&= \begin{cases} 1 & \text{if } \zeta^k = \pm 1, \\ q & \text{otherwise.} \end{cases}
\end{aligned}$$

Therefore we get that the polynomial g satisfies the desired result. \square

4. UNIQUENESS

In this section we study how easy it is for a Littlewood polynomial to satisfy equality of Conjecture 1.1. Specifically, for $f \in \mathcal{L}_N$ (or even $f \in \mathcal{A}_N$), if we have

$$(4.1) \quad |f(\zeta^k)|^2 = \begin{cases} 1 & \text{if } \zeta^k = \pm 1, \\ q & \text{otherwise,} \end{cases}$$

then what properties does f satisfy?

Assume that f satisfies condition (4.1) above. Let $p|N+1$ and let $N|q-1 = p^k - 1$. (If $N+1$ is a power of a prime, then $q = N+1$.) Let ζ be a primitive N th root of unity in \mathbb{C} , and r be a primitive N th root of unity in \mathbb{F}_q . Let $\pi : \mathbb{Z}[\zeta] \rightarrow \mathbb{F}_q$ by $\pi(\zeta) = r$. Note that for any k , with $\frac{N}{2} \nmid k$ we have that $|f(\zeta^k)|^2 = f(\zeta^k)f^*(\zeta^k) = q$. Therefore, in this case $\pi(f(\zeta^k)f(\zeta^{-k})) = 0$, which implies $\bar{f}(r^k)\bar{f}(r^{-k}) = 0$, where $\bar{f} \in \mathbb{F}_q[z]$. For the rest of this section we will focus our attention to polynomials over \mathbb{F}_q , and as such, to simplify notation, we will use f instead of \bar{f} . This gives us that $\{r^{\pm 1}, r^{\pm 2}, \dots, r^{\pm(N/2-1)}\}$ are all roots of $f(z)f^*(z)$, or equivalently that

$$\frac{x^N - 1}{x^2 - 1} \Big| f(z)f^*(z),$$

where all polynomials are elements of $\mathbb{F}_q[z]$. Computationally it seems that we have tighter conditions on the roots most of the times. Namely for most optimal polynomials there exists a primitive N th root of unity r such that $f(r^i) = 0$ for $i = 1, 2, \dots, N/2 - 1$. Of the 700 optimal polynomial found in Section 5, 690 of

them had this property. (There were 2 for $N = 8$ that did not, and 8 for $N = 58$.) See Section 5 for more on the computations.

If we assume that such an r exists, we get

Theorem 4.1. *Let $p|N + 1$ and let $N|q - 1 = p^k - 1$. Let $r \in \mathbb{F}_q$ be a primitive N th root of unity. Assume that $f \in \mathcal{L}_N \subset \mathbb{F}_q[z]$ such that $f(r^i) = 0$ for $i = 1, 2, \dots, N/2 - 1$. Then $q = N + 1$ and $f(z) = \pm \sum \chi(r^i - 1)z^i$.*

Proof. Let

$$\widehat{f}(z) = \sum_{i=0}^{N-1} f(r^{-i})z^i.$$

(This is the Fourier transform of f with respect to r .) If $f(z) = \sum_i a_i z^i$, and $\widehat{f}(z) = \sum_i b_i z^i$, then

$$\begin{aligned} f(r^{-i}) &= b_i, \\ \widehat{f}(r^j) &= Na_j \\ &= -a_j. \end{aligned}$$

Therefore, by our assumptions we get that $\widehat{f} \in \mathbb{F}_q[z]$ of degree at most $N/2$, as $b_{N-i} = f(r^i) = 0$ for $i = 1, 2, \dots, N/2 - 1$. However, since $a_i = \pm 1$ we get that $\widehat{f}(1) = 0$, and $\widehat{f}^2(z) = 1$ for z any root of $(z^N - 1)/(z - 1)$. Therefore

$$\widehat{f}(z)^2 - 1 = \frac{z^N - 1}{z - 1} h(z)$$

for some linear function $h(z)$, since the degree of \widehat{f} is at most $N/2$ we get that \widehat{f}^2 has degree no more than N . Evaluating at 1 we get $\widehat{f}(1)^2 - 1 = Nh(1)$, which implies $h(1) = 1$. Taking the derivative of both sides and evaluating at 1 we get

$$\begin{aligned} 0 = 2\widehat{f}(1)\widehat{f}'(1) &= \left(\frac{d}{dz} \frac{z^N - 1}{z - 1} h(z) \right) \Big|_{z=1} \\ &= \left(\frac{d}{dz} \frac{(1 + (z - 1))^N - 1}{z - 1} h(z) \right) \Big|_{z=1} \\ &= \left(\sum_k \binom{N}{k+1} (z - 1)^k h'(z) + k \binom{N}{k+1} (z - 1)^{k-1} h(z) \right) \Big|_{k=1} \\ &= \left(Nh'(1) + \frac{N(N-1)}{2} \right) h(1) \\ &= h(1) - h'(1), \end{aligned}$$

and hence $h'(1) = 1$. Solving for $h(z)$ we get $h(z) = z$, which implies

$$\widehat{f}(z)^2 = \frac{z^{N+1} - 1}{z - 1}.$$

Let $N + 1 = Mp^\alpha$ where $(M, p) = 1$. We will first prove that $M = 1$. Note that since we are working in characteristic p we get

$$z^{N+1} - 1 = z^{Mp^\alpha} - 1 = (z^M - 1)^{p^\alpha}.$$

However we have

$$\frac{z^{N+1} - 1}{z - 1} = (z - 1)^{p^\alpha - 1} (1 + z + \dots + z^{M-1})^{p^\alpha}$$

is a perfect square. However, $1 + z + \dots + z^{M-1}$ is square free and hence $(1 + z + \dots + z^{M-1})^{p^\alpha}$ is not a perfect square, unless $M = 1$. This proves that $N + 1 = q$, and $\widehat{f}(z)^2 = (z - 1)^N$. This give us $\widehat{f}(z) = \pm(z - 1)^{N/2}$. Hence

$$a_i = -\widehat{f}(r^i) = \pm(r^i - 1)^{N/2} = \pm\chi(r^i - 1)$$

and hence

$$f(z) = \pm \sum \chi(r^i - 1)z^i$$

as desired. \square

Remark 4.2. Note that the only place where we used the assumption that $f(r) = f(r^2) = \dots = f(r^{N/2-1}) = 0$ was to bound the degree of \widehat{f} , or equivalently to show that h is linear. This in turn is sufficient to find exact value for $\widehat{f}(z)^2$. Without this assumption we can find $\widehat{f}(z)^2$ modulo $z^N - 1$, however we do not know how to use this to show $N + 1 = q$.

5. COMPUTATIONAL VERIFICATION OF CONJECTURES & FINAL COMMENTS

We have done extensive computations on the space of Littlewood-like polynomials in support of some of our conjectures. In particular we have

- (1) Constructed all Fekete-like polynomials as given in Theorem 3.1 up to degree $N = 500$.
- (2) Found all $f \in \mathcal{L}_N$, with $N \leq 42$ and all $f \in \mathcal{A}_N$, with $N \leq 84$ such that $\max_i |f(\zeta^i)| = \sqrt{N + 1}$

Given the large number of Fekete-like polynomials up to degree 500, data was only collected on some of them. (There were over 16,616 Fekete-like polynomials of degree up to 500.) In particular, for all Fekete polynomials of degree less than 427 and a random selection of Fekete polynomials of degree less than 500 we compute their maximum value, minimum value, L_4 norm, merit factor, number of real zeros in $[0, 1]$, and number of zeros on $|z| = 1$. In total, we collected data for 14,391 polynomials.

There are a number of observations that are worth making based on this data. First though, it is worth observing a simple

Fact 5.1. *Let $f \in \mathcal{L}_N$, and ζ be a primitive N th root of unity.*

- *If $g(z) = \pm f(\pm z)$ then*

$$\max_i |f(\zeta^i)| = \max_i |g(\zeta^i)|$$

- *Let $\gcd(k, N) = 1$ and $g(x) \equiv f(x^k) \pmod{x^N - 1}$, where $g(x) \in \mathcal{L}_N$. Then*

$$\max_i |f(\zeta^i)| = \max_i |g(\zeta^i)|$$

The proof is left to the interested reader.

The first observation in Fact 5.1 was explicitly used in the second computations. We only searched for those $f \in \mathcal{L}_N$, or \mathcal{A}_N where $f(x) = x + x \pm \dots$. This cut our search space by a factor of 4.

Of the 700 optimal polynomial found, almost all satisfied $f(\pm 1)^2 = 1$. The only exception we found was when $N = 8$, and is given by the polynomial

$$f_8(z) = -x^7 + x^6 - x^5 + x^4 + x^3 + x^2 + x$$

along with the 3 related polynomials given by Fact 5.1. We are not sure if this is the small number phenomenon.

As well, in Theorem 4.1, we assumed that there exists an r , a primitive N th root of unity in \mathbb{F}_q , such that $f(r) = f(r^2) = \dots = f(r^{N/2-1}) = 0$ in \mathbb{F}_q . There are two known exception to the case which are still optimal polynomial. The first is f_8 above. The second is when $N = 58$ and is given by

$$\begin{aligned} f_{58} = & x^{57} - x^{56} - x^{55} + x^{54} + x^{53} + x^{52} + x^{51} + x^{50} + x^{49} + x^{48} - x^{47} \\ & + x^{46} + x^{45} - x^{44} - x^{43} - x^{42} - x^{41} + x^{40} - x^{39} - x^{38} - x^{37} + x^{36} \\ & + x^{35} - x^{34} + x^{33} + x^{32} - x^{31} + x^{30} - x^{29} - x^{28} - x^{27} - x^{26} + x^{25} \\ & + x^{24} + x^{23} - x^{22} - x^{21} + x^{20} - x^{19} - x^{18} - x^{17} + x^{16} - x^{15} + x^{14} \\ & + x^{13} - x^{12} - x^{11} - x^{10} + x^9 - x^8 + x^7 - x^6 + x^5 - x^4 - x^3 + x^2 + x \end{aligned}$$

along with its 7 related polynomials given by Fact 5.1. Here the roots seem to satisfy a much difference property. Namely, if $f(r) \equiv 0 \pmod{59}$ then $f(r^7) \equiv 0 \pmod{59}$. As $\{7^i\} \pmod{58}$ has an orbit of size 7, this partitions the roots of f_{58} into 4 groups of size 7, 14 of which are primitive, and 14 of which are not.

With the exception of f_8 and f_{58} above, and their related polynomials, of the polynomials found, if f is an optimal polynomial then f is a Fekete-like polynomial, as constructed by Theorem 3.1.

In our search for examples of polynomials, we restricted our search to $f \in \mathcal{A}_N$ when $N \geq 44$. When $N \leq 42$, we searched all $f \in \mathcal{L}_N$. In this search for $N \leq 42$, which found 216 polynomials, we did not find any polynomial in $\mathcal{L}_N \setminus \mathcal{A}_N$. We conjecture that all optimal polynomials are anti-skewsymmetric.

In the proof of Theorem 1.3, we needed $f \in \mathcal{A}_N$ to give a lower bound on $\sum c_k^2$. If we allow $f \in \mathcal{L}_N$, we could get all $c_k \equiv 0 \pmod{4}$ for $k \neq 0$, (for example, use $f = x + x^2 + \dots + x^5$), so we cannot use a modular argument to get the desired inequality. It is not clear what methods should be used to replace this method.

It is worth observing that this problem is very reminiscent of a number of problems that come up in the study of Barker polynomials. In these problems, one looks at a sequence of integers $a_0, a_1, \dots, a_{N-1} \in \{\pm 1\}$ and define the $c'_k = \sum_{i-j=k} a_i a_j$. In this paper we are looking at the *cyclic* autocorrelation problem (summing over $i - j \equiv k \pmod{N}$), with $a_0 = 0$, where as the Barker polynomial problem looks at the *acyclic* autocorrelation problem (summing over $i - j = k$) with $a_0 = \pm 1$. See for example [6, 9, 10, 12].

In our proof of Theorem 3.1, we made use of Lemma 3.2. which states that:

$$(5.1) \quad \sum_{a \in \mathbb{F}_q} \chi(a)\chi(a+b) = \begin{cases} -1 & \text{if } b \neq 0, \\ q-1 & \text{if } b = 0. \end{cases}$$

In [7], it is shown that it is possible for this property (5.1) to hold, but for χ not to be a multiplicative function. In fact, they give an explicit example over \mathbb{F}_9 (see Example 2 of [7]). The obvious method of computing $\sum \chi(r^i - 1)x^i$ with these non-multiplicative functions χ does not give us an optimal polynomial. That is partly because in the proof of Theorem 3.1 we also used the fact that χ is a multiplicative function. It is not clear if these non-multiplicative functions are related to other optimal polynomials.

In the proof of Theorem 4.1, we needed to make an extra assumption on the roots of the optimal polynomial over some finite field. This assumption is clearly

too restrictive since there exists other optimal polynomials that don't satisfy the said assumptions. It is not clear if it would be possible to give a more complete description than Theorem 3.1 such that we would have a complete description of all optimal polynomials. Currently as it stands, we don't even know that if equality holds, then $N + 1$ must be a prime power, although all evidences seems to suggest this.

One of the oldest conjectures, of Littlewood, concerning these types of problems is, does there exists C_1 and C_2 , and a family of polynomials h with ± 1 coefficients such that

$$(5.2) \quad C_1 \sqrt{\deg(h)} \leq |h(z)| \leq C_2 \sqrt{\deg(h)}$$

for all $|z| = 1$. For more discussion on this conjecture, see [3]. Proving the easier conjecture, with respect to the upper bound only, looked promising for the Fekete polynomials $h_N(z) = \sum \left(\frac{i}{N}\right) z^i$ for an odd prime N , since $\max_i |h_N(\zeta^i)| = \sqrt{N}$. Unfortunately the values off of these roots of unity is sufficiently large so that the partial conjecture cannot be proved in this way. In particular, with the standard Fekete polynomials, it is known that

$$(5.3) \quad \frac{2}{\pi} \sqrt{N} \log \log(N) < \max_{|z|=1} |h_N(z)| \ll \sqrt{N} \log(N)$$

See [11]. One obvious question from this is, what happens with the Fekete-like polynomials? Can bounds such as (5.3) be found? It clearly cannot satisfy Littlewood's original conjecture, as $f(\pm 1)^2 = 1$ for all Fekete-like polynomials.

Computationally it appears that the maximum grows faster than \sqrt{N} . In fact, it appears that for large N that

$$C_1 \log \log(N) \sqrt{N} < \max_{|z|=1} |f(z)| < C_2 \log \log(N) \sqrt{N}$$

with $C_1 > 0.85$ and $C_2 < 1.45$. This has the same sort of order as the lower bound for Fekete polynomials.

One related questions to this concerns the L_4 norm, or the Merit factor of such polynomials. In [4] a explicit value for the L_4 norm, and Merit factors for Fekete polynomials is given. Recall the L_α norm and Merit factor are defined as

$$\begin{aligned} \|f\|_\alpha &= \left(\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^\alpha d\theta \right)^{1/\alpha} \\ \text{MF}(f) &= \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4} \end{aligned}$$

Here the L_2 norm a polynomials is the square root of the sum of the squares of the coefficients, so in our case $\sqrt{N-1}$. For example, they show that, for h_N a Fekete polynomial that

$$\|h_N\|_4^4 = \frac{5}{3}N^2 - 3N + \frac{4}{3} - 12C(-q)^2$$

where $C(-q)$ is the class number of $\mathbb{Q}(\sqrt{-q})$. The expected value of the L_4 norm of a Littlewood polynomial is $2^{1/4}\sqrt{N}$, which gives a Merit factor of 1. For Fekete polynomials, the asymptotic Merit factor is $3/2$, and if we move to the Turyn polynomials (which are a cyclic shift of the Fekete polynomials) we can get up to a Merit factor of 6. An obvious question is, what happens with Fekete-like polynomials? It appears that the L_4 norm grows like $C\sqrt{N}$ where $1.04 < C < 1.11$.

Computationally it appears that the Merit factors of these polynomials is tending to 3 for large N .

Another property of Fekete polynomials that has been much studied is the locations of their roots. Initially, if we only look at primes less than 1000, there are very few (23 in total) Fekete polynomials that have real roots in the interval $(0, 1)$. This trend does not continue. In particular, Baker and Montgomery [1] show that for almost all large primes N , that the Fekete polynomial h_N has a large number of zeros in this interval. See also [2] for an alternate discussion on this topic. In [8], it is shown that more than half of the roots of Fekete polynomials are on the unit circle. An obvious question is again, what happens with Fekete-like polynomials? Computationally it appears that the Fekete-like polynomials have no roots on the unit circle, ever. The Fekete-like polynomials can have roots in the interval $(0, 1)$, and appears to happen quite often (about $3/4$ of the time). In the other direction, we haven't found any Fekete-like polynomial with more than 5 real root in this interval. Based on the data, it appears likely that the number of roots grows somewhat with N , so it should be possible to find polynomials with an arbitrary number of roots in $[0, 1]$, for large enough N .

REFERENCES

- [1] R. C. Baker and H. L. Montgomery, *Oscillations of quadratic L -functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 23–40.
- [2] Paul T. Bateman, George B. Purdy, and Samuel S. Wagstaff, Jr., *Some numerical results on Fekete polynomials*, Math. Comput. **29** (1975), 7–23, Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.
- [3] Peter Borwein, *Some old problems on polynomials with integer coefficients*, Approximation theory IX, Vol. I. (Nashville, TN, 1998), Vanderbilt Univ. Press, Nashville, TN, 1998, pp. 31–50.
- [4] Peter Borwein and Kwok-Kwong Stephen Choi, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), no. 1, 219–234 (electronic).
- [5] Peter Borwein, Kwok-Kwong Stephen Choi, and Soroosh Yazdani, *An extremal property of Fekete polynomials*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 19–27 (electronic).
- [6] Peter Borwein, Erich Kaltofen, and Michael J. Mossinghoff, *Irreducible polynomials and Barker sequences*, ACM Commun. Comput. Algebra **41** (2007), no. 3-4, 118–121.
- [7] Kwok-Kwong Choi and Man-Keung Siu, *Counter-examples to a problem of Cohn on classifying characters*, J. Number Theory **84** (2000), no. 1, 40–48.
- [8] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 865–889.
- [9] M. Elia, *On the nonexistence of Barker sequences*, Combinatorica **6** (1986), no. 3, 275–278.
- [10] Jonathan Jedwab and Sheelagh Lloyd, *A note on the nonexistence of Barker sequences*, Des. Codes Cryptogr. **2** (1992), no. 1, 93–97.
- [11] Hugh L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.
- [12] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA, N2L 3G1

E-mail address: kghare@math.uwaterloo.ca

DEPARTMENT OF MATHEMATICS, MCMASTER UNIVERSITY, HAMILTON, ONTARIO, CANADA, L8S 4L8

E-mail address: syazdani@math.mcmaster.ca