BARKER SEQUENCES AND FLAT POLYNOMIALS

PETER BORWEIN AND MICHAEL J. MOSSINGHOFF

ABSTRACT. A Barker sequence is a finite sequence of integers, each ± 1, whose aperiodic autocorrelations are all as small as possible. It is widely conjectured that only finitely many Barker sequences exist. We describe connections between Barker sequences and several problems in analysis regarding the existence of polynomials with ± 1 coefficients that remain flat over the unit circle according to some criterion. First, we amend an argument of Saffari to show that a polynomial constructed from a Barker sequence remains within a constant factor of its L_2 norm over the unit circle, in connection with a problem of Littlewood. Second, we show that a Barker sequence produces a polynomial with very large Mahler's measure, in connection with a question of Mahler. Third, we optimize an argument of Newman to prove that any polynomial with ± 1 coefficients and positive degree $n-1$ has L_1 norm less than $\sqrt{n-.09}$, and note that a slightly stronger statement would imply that long Barker sequences do not exist. We also record polynomials with ± 1 coefficients having maximal L_1 norm or maximal Mahler's measure for each fixed degree up to 24. Finally, we show that if one could establish that the polynomials in a particular sequence are all irreducible over $\mathbb{Q}$, then an alternative proof that there are no long Barker sequences with odd length would follow.

1. INTRODUCTION

For a sequence of complex numbers $a_0, a_1, \ldots, a_{n-1}$, define its *aperiodic autocorrelation sequence* $\{c_k\}$ by

$$c_k := \sum_{j=0}^{n-1-k} a_j \overline{a}_{j+k}$$

for $0 \le k < n$ and

$$c_{-k} := \overline{c}_k.$$

We are interested here in the case when the a_j are all of unit modulus, in particular when each $a_j = \pm 1$. Thus the *peak autocorrelation* c_0 has the value $c_0 = n$, and in many applications it is of interest to minimize the *off-peak autocorrelations* $c_{\pm k}$ with $0 < k < n$. In the integer case, clearly the optimal situation occurs when $|c_k| \le 1$ for each $k \ne 0$, so $c_k = 0$ if $2 \mid (n-k)$ and $c_k = \pm 1$ otherwise. A sequence achieving this for each k is called a *Barker sequence*. Barker first asked for ± 1 sequences with this property in 1953 [1]. (In fact, Barker asked for the stricter condition that $c_k \in \{0, -1\}$ for $k \ne 0$.) For the complex unimodular case, we

Date: September 30, 2006.

2000 *Mathematics Subject Classification.* Primary: 11B83, 42A05; Secondary: 30C10, 94A55.

Key words and phrases. Barker sequences, flat polynomials, Littlewood polynomials, Mahler's measure, L_p norm.

Research of P. Borwein supported in part by NSERC of Canada and MITACS.

say $\{a_k\}$ is a *generalized Barker sequence* if each off-peak autocorrelation satisfies $|c_k| \le 1$.

Since negating every other term of a sequence $\{a_k\}$ does not disturb the magnitudes of its autocorrelations, we may assume that $a_0 = a_1 = 1$ in a Barker sequence. With this normalization, just eight Barker sequences are known, all with length at most 13. These are shown in Table 1. (Only three of these satisfy the more strict condition requested by Barker—the ones of length 3, 7, and 11.) It is widely conjectured that no additional Barker sequences exist, and in section 2 we survey some known restrictions on their existence. First however we describe a broader conjecture that arises in signal processing, and an equivalent problem in analysis regarding norms of polynomials.

Sequences with small off-peak autocorrelations are of interest in a number of applications in signal processing and communications (see [1,13,19]). In engineering applications, a common measure of the value of a sequence is the ratio of the square of the peak autocorrelation to the sum of the squares of the moduli of the off-peak values. This is called the *merit factor* of the sequence. For a sequence $A_n = \{a_j\}$ of length n then its merit factor is defined by

$$\mathrm{MF}(A_n) := \frac{n^2}{2\sum_{k=1}^{n-1} |c_k|^2}.$$

Golay introduced this quantity in 1972 [16], and in [17] he conjectured that the merit factor of a binary sequence is bounded, presenting a heuristic argument that $\mathrm{MF}(A_n) < 12.32$ for large n. Several researchers in engineering, physics, and mathematics have made similar conjectures; see for instance [4] or [19]. It is clear, however, that a Barker sequence of length n has merit factor near n, so certainly Golay's merit factor conjecture contains the question of the existence of long Barker sequences as a special case.

TABLE 1. Barker sequences with $a_0 = a_1 = 1$.

n	Sequence	Merit factor
2	++	2.00
3	++−	4.50
4	+++−	4.00
4	++−+	4.00
5	+++−+	6.25
7	+++−−+−	8.17
11	+++−−−+−−+−	12.10
13	+++++−−++−+−+	14.08

The merit factor problem may be restated as a question on polynomials. We first require some notation. Given a sequence $\{a_j\}_{j=0}^{n-1}$, define a polynomial $f(z)$ of degree $n-1$ by

$$f(z) = \sum_{j=0}^{n-1} a_j z^j.$$

For a positive real number p, let $\|f\|_p$ denote the value

$$\|f\|_p := \left(\int_0^1 |f(e(t))|^p \, dt \right)^{1/p},$$

where $e(t) := e^{2\pi i t}$. If $p \geq 1$, this is the usual L_p norm of f on the unit circle. We also let $\|f\|_\infty$ denote the supremum norm of f,

$$\|f\|_\infty := \lim_{p\to\infty} \|f\|_p = \sup_{|z|=1} |f(z)|,$$

and we let $\|f\|_0$ denote its geometric mean on the unit circle,

$$\|f\|_0 := \lim_{p\to 0+} \|f\|_p = \exp\left(\int_0^1 \log|f(e(t))|\, dt\right).$$

This is *Mahler's measure* of the polynomial. We recall that if $p < q$ are positive real numbers and f is not a monomial, then

$$\|f\|_0 < \|f\|_p < \|f\|_q < \|f\|_\infty.$$

Assuming that $|a_j| = 1$ for each j, we have $\|f\|_2^2 = n$ by Parseval's formula, and, since $\overline{z} = 1/z$ on the unit circle, it is easy to see that

$$\|f\|_4^4 = \left\|f(z)\overline{f(z)}\right\|_2^2 = \left\|\sum_{k=1-n}^{n-1} c_k z^k\right\|_2^2 = n^2 + 2\sum_{k=1}^{n-1} |c_k|^2. \tag{1.1}$$

Thus, the merit factor of a sequence $\{a_j\}$ can be expressed in terms of certain L_p norms of its associated polynomial,

$$\mathrm{MF}(f) := \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4}.$$

Golay's problem on maximizing the merit factor of a family of sequences of fixed length is thus equivalent to minimizing the L_4 norm of a collection of polynomials of fixed degree. This latter problem is one instance of a family of questions regarding the existence of so-called *flat polynomials*.

For a positive integer n, let $\mathfrak{U}_n$ denote the set of polynomials in $\mathbb{C}[x]$ defined by

$$\mathfrak{U}_n := \left\{ f(z) = \sum_{j=0}^{n-1} a_j z^j : |a_j| = 1 \text{ for } 0 \leq j < n \right\},$$

and let $\mathfrak{L}_n$ denote the subset

$$\mathfrak{L}_n := \left\{ f(z) = \sum_{j=0}^{n-1} a_j z^j : a_j = \pm 1 \text{ for } 0 \leq j < n \right\}.$$

We call the first set the *unimodular polynomials* of degree $n-1$, and the second set the *Littlewood polynomials* of fixed degree. In 1966, Littlewood [23] asked about the existence of polynomials in these sets with particular flatness properties. More precisely, he asked if there exist absolute positive constants α_1 and α_2 and arbitrarily large integers n such that there exists a polynomial $f_n \in \mathfrak{U}_n$ (or, more strictly, $f_n \in \mathfrak{L}_n$), where

$$\alpha_1\sqrt{n} \leq |f_n(z)| \leq \alpha_2\sqrt{n}$$

for all z with $|z| = 1$. Since each polynomial in such a sequence never strays far from its L_2 norm, we say such a sequence is *flat*. In 1980, Körner [21] established that flat sequences of unimodular polynomials exist, and in the same year Kahane [20] proved moreover that for any $\epsilon > 0$ there exists a flat sequence of unimodular polynomials with $\alpha_1 = 1 - \epsilon$ and $\alpha_2 = 1 + \epsilon$. Such sequences are often called *ultraflat*.

Much less is known regarding flat sequences of Littlewood polynomials. The Rudin-Shapiro polynomials [28,31] satisfy the upper bound in the flatness condition with $\alpha_2 = \sqrt{2}$, but no sequence is known that satisfies the lower bound. In fact, the best known result here is due to Carrol, Eustice, and Figiel [8], who used the Barker sequence of length 13 to show that for sufficiently large n there exist polynomials $f_n \in \mathfrak{L}_n$ with $|f_n(z)| > n^{.431}$ on $|z| = 1$. Also, in 1962 Erdős [12] conjectured that ultraflat Littlewood polynomials do not exist, opining that there exists an absolute positive constant ϵ such that

$$\frac{\|f\|_\infty}{\|f\|_2} > 1 + \epsilon$$

for every Littlewood polynomial of positive degree. (Littlewood however [23, sec. 6; 24, prob. 19] in effect conjectured that no such ϵ exists.) Since $\|f\|_4 \le \|f\|_\infty$, we see then that Golay's merit factor problem is in fact a stronger version of Erdős' conjecture. Further, from (1.1) it follows that if the coefficients of f form a Barker sequence of length n, then

$$\frac{\|f\|_4}{\sqrt{n}} \le \left(1 + \frac{1}{n}\right)^{1/4} < 1 + \frac{1}{4n}.$$

Therefore, to show that long Barker sequences do not exist, it would suffice to prove that $\|f\|_4 \ge \sqrt{n} + \frac{1}{4\sqrt{n}}$ for $f \in \mathfrak{L}_n$ and n large. Similar observations occur for example in [6, chap. 14] and [7].

In this paper, we describe some further connections between Barker sequences and flatness problems for polynomials. Section 2 summarizes some known results on Barker sequences. Section 3 shows that long Barker sequences provide an answer to Littlewood's question on flat polynomials, amending an argument of Saffari that connects these two problems. Section 4 then ties the existence of long Barker sequences to a problem of Mahler's concerning Littlewood polynomials with large measure. Section 5 connects the Barker sequence question to problems on the L_1 norm of Littlewood polynomials, and optimizes an argument of Newman to provide an improved restriction on the flatness of Littlewood polynomials with respect to this norm. Finally, section 6 outlines a possible alternative method for establishing that there are no Barker sequences of certain lengths.

2. Barker sequences

We first record some facts about Barker sequences. The following results are due to Turyn and Storer [32,33]; we include the proof here for the reader's convenience.

Theorem 2.1. *Suppose a_0, a_1, ..., a_{n-1} is a sequence of integers with each $a_i = \pm 1$, and let $\{c_k\}$ denote its aperiodic autocorrelations. Then*

$$c_k + c_{n-k} \equiv n \mod 4.$$

If in addition the sequence $\{a_k\}$ is a Barker sequence, then

$$a_k a_{n-1-k} = (-1)^{n-1-k}.$$

If furthermore n is even and $n > 2$, then $n = 4m^2$ for some integer m, and $c_{n-k} = -c_k$ for $0 < k < n$. If n is odd, then $c_k + c_{n-k} = (-1)^{(n-1)/2}$ for each k.

Proof. Since c_k records the difference between the number positive and negative terms in $\sum_{i=0}^{n-1-k} a_i a_{i+k}$, it follows that

$$\prod_{i=0}^{n-k-1} a_i a_{i+k} = (-1)^{(n-k-c_k)/2} \tag{2.1}$$

for $0 \le k \le n$. Multiplying this product by the same expression with k replaced by $n-k$, we obtain

$$(-1)^{(n-c_k-c_{n-k})/2} = \prod_{i=0}^{k-1} a_i a_{i+n-k} \prod_{i=0}^{n-k-1} a_i a_{i+k} = 1,$$

so $c_k + c_{n-k} \equiv 0 \bmod 4$. Assume now that $\{a_k\}$ forms a Barker sequence of length n. Multiplying (2.1) by the same equation with k replaced by $k+1$, we compute that

$$a_k a_{n-1-k} = (-1)^{n-1-k}.$$

Also, certainly $c_k = 0$ if $0 < k < n$ and $n \equiv k \bmod 2$, and $c_k = \pm 1$ for the other k in this range. In particular, if n is even and $n > 2$, then $c_2 + c_{n-2} = 0$, so $n \equiv 0 \bmod 4$. It follows then that $c_k + c_{n-k} = 0$ for $0 < k < n$ in this case. Last, since

$$\left(\sum_{i=0}^{n-1} a_i\right)^2 = c_0 + \sum_{k=1}^{n-1} (c_k + c_{n-k}) = n,$$

we see that n is a perfect square if $n \ge 4$ is even. □

Recall that a polynomial $f(z)$ with integer coefficients is *skew-symmetric* if $f(z) = \pm z^{\deg f} f(-1/z)$. We remark that Theorem 2.1 then shows that every Barker sequence of odd length corresponds to a skew-symmetric Littlewood polynomial.

Much more is known about possible lengths of Barker sequences. Turyn and Storer [32] proved that if the length n of a Barker sequence is odd then $n \le 13$, so the complete list for this case appears in Table 1. It also follows from this that no additional sequences satisfy Barker's original requirement for sequences whose off-peak autocorrelations are all 0 or -1, since Theorem 2.1 implies that any such sequence must have length $n \equiv 3 \bmod 4$. For the even case, we write $n = 4m^2$. In 1965 Turyn [34] showed in effect that m must be odd and cannot be a prime power (see also [2, sec. 2D and 4C; 10, 11]). In 1990, Eliahou, Kervaire, and Saffari [9] proved that if $p \mid m$ then $p \equiv 1 \bmod 4$; in 1992 Eliahou and Kervaire [10] and Jedwab and Lloyd [18] both used this constraint, together with some additional restrictions on m, to show that there are no Barker sequences with $1 < m < 689$. In 1999, Schmidt [30] obtained much stronger restrictions on m, determining that no Barker sequences exist with $m \le 10^6$. This method was refined and extended by Leung and Schmidt in 2005 [22], who established that no Barker sequences exist with $1 < m \le 5 \cdot 10^{10}$, that is, with even length n satisfying $4 < n \le 10^{22}$. Another restriction was obtained in 1989 by Fredman, Saffari, and Smith [15], who proved that a Barker sequence may not be palindromic.

3. Littlewood's problem

In 1990, Saffari [29] noted that if there are in fact infinitely many Barker sequences, then Littlewood's conjecture on the existence of flat polynomials with ± 1 coefficients follows. We present Saffari's proof here, in part because we require the

result in section 3, but also to correct an oversight in the original article. The correction here affects the values of the constants in the following theorem.

Theorem 3.1. *Suppose f is a Littlewood polynomial of degree $n-1$ whose sequence of coefficients $\{a_k\}$ forms a Barker sequence of length n. Then*

$$\alpha_1 + O\left(\frac{1}{n}\right) \le \frac{|f_n(z)|}{\sqrt{n}} \le \alpha_2 + O\left(\frac{1}{n}\right)$$

for each z of modulus 1, where $\alpha_1 = \sqrt{1-\theta} = 0.52477485\ldots$, $\alpha_2 = \sqrt{1+\theta} = 1.31324459\ldots$, and

$$\theta = \sup_{t>0} \frac{\sin^2 t}{t} = 0.7246113537\ldots.$$

Proof. Suppose $f \in \mathfrak{L}_n$ with $n > 13$, and write $n = 4m$. Using the fact that the off-peak autocorrelations satisfy $c_{n-k} = -c_k$ from Theorem 2.1, and that $c_{2j} = 0$ for $j \ge 1$, we compute

$$\begin{aligned}
\left|f\left(e^{it}\right)\right|^2 - n &= 2\sum_{k=1}^{n-1} c_k \cos kt \\
&= 2\sum_{k=1}^{2m-1} c_k\big(\cos kt - \cos((n-k)t)\big)\big) \\
&= 4\sin(2mt)\sum_{k=1}^{2m-1} c_k \sin((2m-k)t) \\
&= 4\sin(2mt)\sum_{k=1}^{m} c_{2m-2k+1}\sin((2k-1)t).
\end{aligned}$$

Thus

$$\left|\frac{\left|f\left(e^{it}\right)\right|^2}{n} - 1\right| \le \theta_m, \tag{3.1}$$

where θ_m is defined by

$$\theta_m := \max_{0\le t<2\pi} \frac{|\sin(2mt)|}{m}\sum_{k=1}^{m} |\sin((2k-1)t)|\,.$$

Define ϕ_m and ψ_m by

$$\phi_m := \max_{0\le t\le \pi/4} \frac{|\sin(2mt)|}{m}\sum_{k=1}^{m} |\sin((2k-1)t)|$$

and

$$\psi_m := \max_{0\le t\le \pi/4} \frac{|\sin(2mt)|}{m}\sum_{k=1}^{m} |\cos((2k-1)t)|\,,$$

so that $\theta_m = \max\{\phi_m, \psi_m\}$. For ϕ_m, note first that the quantity

$$\frac{1}{m}\sum_{k=1}^{m} |\sin((2k-1)t)|$$

is the midpoint approximation over m subintervals of equal size for the integral

$$\int_0^1 |\sin(2mtx)|\,dx.$$

We consider the error incurred when approximating this integral with the sum over each interval $[(k-1)/m, k/m]$. If no cusp occurs in the interval, certainly the error is at most $1/24m^3$, so the total error incurred from these intervals is $O(1/m^2)$. If a cusp occurs in an interval, in the worst case it lies at the midpoint, and the ratio of the error incurred in this case to the error when the cusp occurs at an endpoint is $\tan(t/2)/(t-\sin t)$. If $\pi/\sqrt{m} \le t \le \pi/4$, this ratio is $3m/\pi^2 + O(1)$, so the total error incurred on the intervals with cusps is

$$O\left(\frac{3m}{\pi^2}\cdot\frac{1}{24m^3}\cdot\frac{m}{2}\right) = O\left(\frac{1}{m}\right).$$

If $0 \le t < \pi/\sqrt{m}$, then there are at most $2\sqrt{m}$ cusps, and the error in the worst case at each cusp is $(2-\cos(\pi/\sqrt{m}))/2\pi\sqrt{m}$, so the total error in this case is also $O(1/m)$. Therefore,

$$\begin{aligned}
\phi_m &= \max_{0\le t\le \pi/4} |\sin(2mt)| \int_0^1 |\sin(2mtx)|\,dx + O\left(\frac{1}{m}\right)\\
&\le \sup_{\alpha\ge 0} |\sin\alpha| \int_0^1 |\sin(\alpha t)|\,dt + O\left(\frac{1}{m}\right)\\
&= \sup_{n\ge 0} \max_{0\le x\le \pi} \frac{(2n+1-\cos x)\sin x}{n\pi + x} + O\left(\frac{1}{m}\right) \qquad (3.2)\\
&= \max_{0\le x\le \pi} \frac{(1-\cos x)\sin x}{x} + O\left(\frac{1}{m}\right)\\
&= 0.6639534894\ldots + O\left(\frac{1}{m}\right).
\end{aligned}$$

In the same way,

$$\begin{aligned}
\psi_m &= \max_{0\le t\le \pi/4} |\sin(2mt)| \int_0^1 |\cos(2mtx)|\,dx + O\left(\frac{1}{m}\right)\\
&\le \sup_{\alpha\ge 0} |\sin\alpha| \int_0^1 |\cos(\alpha t)|\,dt + O\left(\frac{1}{m}\right)\\
&= \sup_{n\ge 0} \max_{-\frac{\pi}{2}\le x\le \frac{\pi}{2}} \frac{(2n+\sin x)\,|\sin x|}{n\pi + x} + O\left(\frac{1}{m}\right) \qquad (3.3)\\
&= \max_{0\le x\le \frac{\pi}{2}} \frac{\sin^2 x}{x} + O\left(\frac{1}{m}\right)\\
&= 0.7246113537\ldots + O\left(\frac{1}{m}\right).
\end{aligned}$$

The statement then follows from (3.1), (3.2), and (3.3). □

We remark that Saffari computed the limiting value of θ_m to be $0.66395\ldots$ by considering only computation of ϕ_m above for $0 \le t \le 2\pi$. However, this argument breaks down when t is very close to $\pi/2$ or $3\pi/2$.

4. Mahler's problem

In 1963, Mahler [25] posed the question of maximizing the normalized measure $\|f\|_0 / \|f\|_2$ of polynomials with complex coefficients and fixed degree. He proved that for each degree the maximum is attained by a unimodular polynomial, and Fielding [14] proved that there exist unimodular polynomials with normalized measure arbitrarily close to 1. Beller and Newman [3] proved further that there exists a positive constant c such that for each $n > 0$ there exists a polynomial $f_n \in \mathfrak{U}_n$ such that $\|f_n\|_0 > \sqrt{n} - c \log n$. The problem remains open for Littlewood polynomials; the largest known normalized measure in this case is $0.98636598\ldots$, achieved by the polynomial whose coefficients form the Barker sequence of length 13. We prove here that long Barker sequences would also provide an answer to Mahler's problem for the case of Littlewood polynomials.

Theorem 4.1. *Let f_n be a Littlewood polynomial whose coefficients form a Barker sequence of length n. Then*

$$\frac{\|f_n\|_0}{\sqrt{n}} > 1 - \frac{1}{\sqrt{n}}$$

for sufficiently large n.

Proof. Let $f_n(z) = \sum_{j=0}^{n-1} a_j z^j$, with $\{a_j\}$ a Barker sequence. Since the off-peak autocorrelation c_k is 0 if $n \equiv k \bmod 2$ and ± 1 otherwise, it follows from (1.1) that

$$\|f_n\|_4^4 = n^2 + n - \epsilon(n),$$

where $\epsilon(n) = 0$ if n is even and 1 if n is odd. Thus

$$\int_0^1 \left(\frac{|f_n(e(t))|^2}{n} - 1 \right)^2 dt = \frac{\|f_n\|_4^4}{n^2} - 1 = \frac{n - \epsilon(n)}{n^2}.$$

Next, if $a > b > 0$ it is straightforward to verify that

$$\frac{a-b}{b} \geq \log a - \log b,$$

so setting $a(t) = \max\{1, \frac{|f_n(e(t))|^2}{n}\}$ and $b(t) = \min\{1, \frac{|f_n(e(t))|^2}{n}\}$ for t in $[0,1]$, we obtain

$$\int_0^1 \left(\frac{|f_n(e(t))|^2}{n} - 1 \right)^2 dt \geq \int_0^1 \min\left\{ \frac{|f_n(e(t))|^2}{n}, 1 \right\}^2 \left(2 \log |f_n(e(t))| - \log n\right)^2 dt,$$

so

$$\int_0^1 \left(2 \log |f_n(e(t))| - \log n\right)^2 dt \leq \frac{1}{\alpha_1^2 n} + O\left(\frac{1}{n^2}\right),$$

where $\alpha_1 = 0.52477\ldots$ is the constant appearing in statement of Theorem 3.1. By the Schwarz inequality,

$$\int_0^1 \left|2 \log |f_n(e(t))| - \log n\right| dt \leq \frac{1}{\alpha_1 \sqrt{n}} + O\left(\frac{1}{n^{3/2}}\right),$$

and so

$$\int_0^1 \log |f_n(e(t))| \, dt \geq \log \sqrt{n} - \frac{1}{2\alpha_1 \sqrt{n}} + O\left(\frac{1}{n^{3/2}}\right).$$

Since $1/2\alpha_1 = 0.9527\ldots$, it follows then that

$$\frac{\|f_n\|_0}{\sqrt{n}} \geq 1 - \frac{1}{2\alpha_1\sqrt{n}} + O\left(\frac{1}{n^{3/2}}\right) > 1 - \frac{1}{\sqrt{n}}$$

for sufficiently large n. □

For each $n \leq 25$, Table 2 lists a Littlewood polynomial with degree $n-1$ having maximal Mahler's measure over $\mathfrak{L}_n$. We remark that the coefficient sequences for $n = 2$, 3, 4, 5, 7, 11, and 13 are precisely the Barker sequences. (The two Barker sequences of length 4 correspond to polynomials with identical Mahler's measure.)

TABLE 2. Maximal Mahler's measure of Littlewood polynomials by degree.

n	Coefficients of f	$\|f\|_0$	$\|f\|_0/\sqrt{n}$	$\sqrt{n} - \|f\|_0$
2	++	1.00000	0.70711	0.41421
3	++−	1.61803	0.93417	0.11402
4	+++−	1.83929	0.91964	0.16071
5	+++−+	2.15372	0.96317	0.08235
6	++++−+	2.22769	0.90945	0.22180
7	+++−−+−	2.49670	0.94366	0.14905
8	++++−−+−	2.64209	0.93412	0.18634
9	+++−+−−++	2.72501	0.90834	0.27499
10	++++−+−−++	2.92076	0.92363	0.24152
11	+++−−−+−−+−	3.16625	0.95466	0.15038
12	++++−−++−+−	3.33463	0.96262	0.12948
13	++++−−++−+−+	3.55639	0.98637	0.04916
14	++++−−++−+−+	3.57536	0.95556	0.16630
15	++++−−++−−+−+−	3.74089	0.96589	0.13209
16	+++−+++−−−+−++−+	3.77645	0.94411	0.22355
17	++−++−−++++−+−+−−	3.87848	0.94067	0.24463
18	+++−+++−−−+−++−+−−	4.01406	0.94612	0.22858
19	++−+−−−+−+++−++++−	4.16269	0.95499	0.19621
20	+++++−+−−−+−++−−++−	4.30167	0.96188	0.17047
21	++−−−−−−−++−−+−+−+−−+	4.39853	0.95984	0.18405
22	+++++−++−−+−+−++−−+++	4.47518	0.95411	0.21523
23	+++++++−−−++−−+−−+−+−+−	4.57183	0.95329	0.22400
24	++−−+++−−−−−+−+−+−−+−−+	4.71462	0.96237	0.18436
25	+++−−−+++++++−+−+−−+−−++−	4.83413	0.96683	0.16587

5. Newman's problem

One may also study flatness properties of polynomials by using the L_1 norm. In this case, again the problem is largely resolved for unimodular polynomials, and largely open for Littlewood polynomials. For the unimodular case, in 1965 Newman [27] proved that there exists a positive constant c so that for each $n \geq 2$ there exists a polynomial $f_n \in \mathfrak{U}_n$ so that $\|f\|_1 > \sqrt{n} - c$. In his proof, Newman first constructed a polynomial f_n whose L_4 norm satisfies $\|f_n\|_4/\sqrt{n} = 1 + O(1/\sqrt{n})$, then used Hölder's inequality to obtain a lower bound on $\|f_n\|_1$ of the desired form.

Much less is known for the Littlewood case. In [26], Newman mentioned a conjecture (without attribution) for the L_1 norm for these polynomials, similar to Erdős' conjecture for the supremum norm: There exists a positive constant $c < 1$ so that $\|f\|_1 < c\sqrt{n}$ whenever $f \in \mathfrak{L}_n$ and $n \geq 2$. This problem remains open, as does the weaker question of whether there exists a positive constant c so that $\|f\|_1 < \sqrt{n} - c$ for $f \in \mathfrak{L}_n$ of positive degree. Resolving a still weaker problem however suffices for answering the question of the existence of Barker sequences of large degree.

Theorem 5.1. *If $f(z) = \sum_{k=0}^{n-1} a_j z_j$ is a Littlewood polynomial whose coefficients form a Barker sequence of length n, then $\|f\|_1 > \sqrt{n-1}$.*

Proof. Suppose $f \in \mathfrak{L}_n$ has coefficients forming a Barker sequence. From (1.1) we see that

$$\|f\|_4^4 = n^2 + n - \epsilon(n),$$

where $\epsilon(n) = 1$ if n is odd and 0 if n is even. Using Hölder's inequality, we have

$$\|f\|_2^2 < \|f\|_1^{2/3} \|f\|_4^{4/3},$$

and so

$$\|f\|_1^2 > \frac{n^3}{n^2 + n - \epsilon(n)} = n - 1 + \frac{1}{n+1}\left(1 + \frac{\epsilon(n) n^2}{n^2 + n - 1}\right). \qquad \square$$

This statement in fact appears in the 1968 paper of Turyn [35], who attributes the observation to Newman.

Newman in fact proved a statement similar to Theorem 5.1 in 1960 [26], showing that $\|f\|_1 > \sqrt{n - .03}$ for $f \in \mathfrak{L}_n$ of positive degree. We revisit Newman's argument here, choosing parameters in an optimal way and employing the results of some computations on Littlewood polynomials to obtain an improved lower bound. It is clear from the proof however that a new approach is needed to obtain the constant 1, as Newman observed.

Theorem 5.2. *If f is a Littlewood polynomial of positive degree $n - 1$, then*

$$\|f\|_1 < \sqrt{n - .09}.$$

Proof. Let $f(z) = \sum_{k=0}^{n-1} a_k z^k$ with $a_k = \pm 1$ for $0 \leq k < n$, and let $\alpha > 1$ be a real number whose value will be selected later. The argument splits into two cases, depending on the size of $\|f\|_\infty$.

Case 1: $\|f\|_\infty \leq \alpha\sqrt{n}$**.** Let c_k denote the kth aperiodic autocorrelation of the sequence of coefficients of f. Since $\sum_{k=1}^{n-1} c_k^2 \geq \lfloor n/2 \rfloor$, using (1.1) we have

$$\|f\|_4^4 \geq n^2 + n - \epsilon(n),$$

where $\epsilon(n) = 1$ if n is odd and 0 otherwise. Next, since

$$\int_0^1 \left(|f(e(t))|^2 - n\right)^2 dt = \|f\|_4^4 - 2n\|f\|_2^2 + n^2 \geq n - \epsilon(n),$$

we compute

$$\int_0^1 \left(|f(e(t))| - \sqrt{n}\right)^2 dt = \int_0^1 \left(\frac{|f(e(t))|^2 - n}{|f(e(t))| + \sqrt{n}}\right)^2 dt \geq \frac{n - \epsilon(n)}{(\alpha+1)^2 n}.$$

However,

$$\int_0^1 \left(|f(e(t))| - \sqrt{n}\right)^2 dt = 2n - 2\sqrt{n}\,\|f\|_1,$$

so

$$\begin{aligned}\|f\|_1^2 &\le n - \frac{n-\epsilon(n)}{(\alpha+1)^2 n} + \frac{(n-\epsilon(n))^2}{4(\alpha+1)^4 n^3} \\ &= n - \frac{1}{(\alpha+1)^2} + O(1/n).\end{aligned} \tag{5.1}$$

Case 2: $\|f\|_\infty > \alpha\sqrt{n}$**.** Suppose $\max_{|z|=1}|f(z)| = A\sqrt{n}$, occurring at $z = e(t_0)$. By Bernstein's inequality, $|f'(z)| \le A(n-1)\sqrt{n}$, so for $0 \le t \le 1$, it follows that

$$|f(e(t))| \ge A\sqrt{n}\big(1 - 2\pi(n-1)\,|t - t_0|\big).$$

Let β be a small positive number whose value will be selected later, let I denote the interval $[t_0 - \beta/n, t_0 + \beta/n]$, and let $B = \int_I |f(e(t))|^2\,dt$. Then

$$\begin{aligned}B &\ge 2\alpha^2 n \int_{t_0}^{t_0+\beta/n} \big(1 - 2\pi(n-1)(t-t_0)\big)^2\,dt \\ &= 2\alpha^2\beta\left(1 - 2\pi\beta\left(1 - \frac{1}{n}\right) + \frac{4\pi^2\beta^2}{3}\left(1 - \frac{1}{n}\right)^2\right).\end{aligned} \tag{5.2}$$

It follows that

$$B \ge 2\alpha^2\beta\left(1 - 2\pi\beta + 4\pi^2\beta^2/3\right) \tag{5.3}$$

if $\beta < 3/4\pi$.

Next, let J denote the complement of I (modulo 1) in $[0,1]$ so that

$$\int_J |f(e(t))|^2\,dt = n - B.$$

By the Schwarz inequality,

$$\left(\int_I |f(e(t))|\,dt\right)^2 \le 2\beta B/n$$

and

$$\left(\int_J |f(e(t))|\,dt\right)^2 \le (n-B)(1 - 2\beta/n),$$

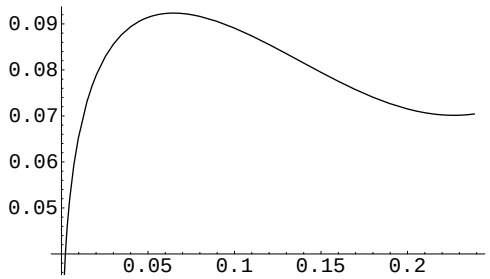
so

$$\|f\|_1 \le \sqrt{2\beta B/n} + \sqrt{(n-B)(1-2\beta/n)}. \tag{5.4}$$

The expression on the right is decreasing in B for $B \ge 2\beta$, so assuming that $\alpha^2(1 - 2\pi\beta + 4\pi^2\beta^2/3) \ge 1$, we may replace B in (5.4) with the expression in (5.3) to obtain

$$\begin{aligned}\|f\|_1^2 \le{}& \Big(2\alpha\beta\sqrt{(1 - 2\pi\beta + 4\pi^2\beta^2/3)/n} \\ &+ \sqrt{(n - 2\alpha^2\beta(1 - 2\pi\beta + 4\pi^2\beta^2/3))(1 - 2\beta/n)}\Big)^2 \\ ={}& n - 2\beta\left(1 + \alpha^2 - 2\alpha^2\beta\pi + 4\alpha^2\beta^2\pi^2/3 - 2\alpha\sqrt{1 - 2\beta\pi + 4\beta^2\pi^2/3}\right) \\ &+ O(1/n).\end{aligned} \tag{5.5}$$

FIGURE 1. Optimal constant term.



Selecting parameters. Now we wish to choose α and β, subject to the identified constraints, so that the constant terms in the expressions (5.1) and (5.5) match and are as large as possible. (Newman uses $\alpha = 2\sqrt{\pi} \approx 3.54$, $\beta = 1/4\pi \approx .0796$, and $B \geq 1$, which yields .0484 in case 1 and .361 in case 2). Selecting candidate values for β between 0 and $3/4\pi$ produces the values of $1/(\alpha+1)^2$ shown in Figure 1. The optimal value is approximately .092347, occurring near $\alpha = 2.2907$ and $\beta = .064804$.

When n is even, we obtain from (5.1) that $\|f\|_1^2 \leq n - .091281$, and it is straightforward to verify that the bound in (5.5) is slightly smaller for all n. However, for odd $n \geq 3$ we obtain from (5.1) that $\|f\|_1^2 \leq n - .09$ only for $n \geq 41$. To obtain the inequality for all odd n, we first perform the analysis a bit more carefully to decrease this threshold, then we complete the proof by determining for small n the maximal value of the L_1 norm of a Littlewood polynomial of degree $n-1$. To this end, we replace the parameter α with the expression $\alpha - \gamma/n$ and use the more precise lower bound from (5.2) for B in (5.4) in place of the bound (5.3). Choosing $\gamma = .899634$ to balance the $1/n$ terms in the respective asymptotic expansions, we verify that both (5.1) and (5.4) yield $\|f\|_1^2 < n - .09$ when n is odd for $n \geq 21$.

To complete the proof, we therefore need only check that every Littlewood polynomial with even degree $n - 1 \leq 18$ satisfies $\|f\|_1 < \sqrt{n - .09}$. This is established in Table 3, which displays for each $n \leq 25$ a Littlewood polynomial of degree $n-1$ having maximal L_1 norm. □

We remark that the last column of the table shows that the value of .09 in Theorem 5.2 cannot in general be replaced with any number larger than .1856.... We also note that the extremal polynomials with respect to the L_1 norm in Table 3 are precisely the same as the extremal Littlewood polynomials with respect to Mahler's measure in Table 2. In particular, the coefficient sequences appearing in Table 3 for $n = 2$, 3, 4, 5, 7, 11, and 13 are Barker sequences. Again, the other Barker sequence of length 4 has the same L_1 norm as that of the $n = 4$ entry in the table.

6. An irreducibility question

As we noted in section 2, Turyn and Storer [32] proved that no Barker sequences of odd length n exist for $n > 13$. Their proof is elementary, though somewhat complicated, and relies on showing that long Barker sequences of odd length must exhibit certain patterns. We describe here a possible alternative route to proving

TABLE 3. Maximal L_1 norms of Littlewood polynomials by degree.

n	Coefficients of f	$\|f\|_1$	$\|f\|_1/\sqrt{n}$	$n - \|f\|_1^2$
2	++	1.27324	0.90032	0.37886
3	++−	1.67761	0.96857	0.18562
4	+++−	1.92555	0.96277	0.29227
5	+++−+	2.19412	0.98124	0.18583
6	++++−+	2.33899	0.95489	0.52912
7	+++−−+−	2.58397	0.97665	0.32311
8	++++−−+−	2.73681	0.96761	0.50989
9	+++−+−−++	2.87385	0.95795	0.74097
10	++++−+−−++	3.04989	0.96446	0.69817
11	+++−−−+−−+−	3.25835	0.98243	0.38317
12	++++++−++−+−	3.40074	0.98171	0.43498
13	++++++−++−+−+	3.57946	0.99276	0.18749
14	+++++++−++−+−+	3.65775	0.97757	0.62088
15	++++++−++−−+−+−	3.80732	0.98305	0.50430
16	+++−++++−−+−++−+	3.89389	0.97347	0.83764
17	++−++−−++++−+−+−−	4.00380	0.97106	0.96956
18	+++−++++−−+−++−+−−	4.13097	0.97368	0.93505
19	++−+−−−+−++++−++++−	4.26105	0.97755	0.84344
20	+++++−+−−−+−++−−−++−	4.39129	0.98192	0.71659
21	++−−−−−−−++−−+−+−+−−+	4.50012	0.98201	0.74893
22	+++++−++−−−+−+−++−−−+++	4.58809	0.97818	0.94943
23	+++++++−−−++−−+−−+−+−+−	4.68409	0.97670	1.05934
24	++−−+++−−−−−−+−+−+−−+−−+	4.81295	0.98244	0.83550
25	+++−−−+++++++−+−+−−−+−−++−	4.92189	0.98438	0.77497

this result, in the hope of spurring further research. The material in this section also appears in [5].

For a polynomial $f(x)$, we define its *reciprocal polynomial* $f^*(x)$ by $f^*(x) := x^{\deg f} f(1/x)$. For $f(x) \in \mathbb{Z}[x]$, we say f is *reciprocal* if $f = \pm f^*$.

Theorem 6.1. *If the polynomial*

$$g_m(x) := \sum_{k=1}^{m} \left(x^{2m-2k} + x^{2m+2k}\right) + (-1)^m (2m+1) x^{2m}$$

is irreducible, then no Barker sequence of length $2m+1$ *exists.*

Proof. Suppose $\{a_k\}$ is a Barker sequence of length $2m+1$, and let $f_m(x) = \sum_{k=0}^{2m} a_k x^k$. By Theorem 2.1, the aperiodic autocorrelation c_k is 0 if k is odd and $(-1)^m$ if $k \neq 0$ and k is even. Thus

$$\begin{aligned} f_m(x) f_m^*(1/x) &= \sum_{k=-m}^{m} c_{2k} x^{2k+2m} \\ &= (2m+1)x^{2m} + \sum_{k=1}^{m} (-1)^m \left(x^{2m+2k} + x^{2m-2k}\right), \end{aligned}$$

and so $g_m(x) = (-1)^m f_m(x) f_m^*(x)$. □

The polynomials $g_m(x)$ are in fact irreducible for $6 < m \le 750$, and it would be interesting if there is a short proof of this for large m. We note however that Erich Kaltofen has observed that the polynomials $g_m(x)$ are in fact always reducible mod p, for any prime p. With his permission, we include his proof of the following more general statement.

Theorem 6.2. *Suppose $f(x)$ is an even, reciprocal polynomial with integer coefficients and $\deg(f) \ge 4$. Then $f(x)$ is reducible mod p for every prime p.*

Proof. If $f = -f^*$ then $f(\pm 1) = 0$ so f is reducible over $\mathbb{Q}$. If $f = f^*$ and $\deg(f) = 4n+2$ then $f(\pm i) = 0$, so again f is reducible over $\mathbb{Q}$ for $n \ge 1$. Suppose then that $f = f^*$ and $\deg(f) = 4n$ with $n \ge 1$, and write $f(x) = g(x^2)$. Clearly $f(x) \equiv g(x)^2 \bmod 2$, so suppose p is an odd prime, and $g(x)$ is irreducible mod p. Let α be a root of g in its splitting field $\mathbb{F}_{p^{2n}}$ over $\mathbb{F}_p$, so that

$$g(x) = \prod_{k=0}^{2n-1} \left(x - \alpha^{p^k}\right).$$

Let γ be a primitive element of $\mathbb{F}_{p^{2n}}$, and let $\alpha = \gamma^t$ for some integer t. Since g is reciprocal, α^{-1} is also a root of g, so $\alpha^{-1} = \gamma^{-t} = \alpha^{p^j} = \gamma^{tp^j}$ for some positive integer $j < 2n$. Then $\gamma^{tp^{2j}} = \gamma^{-tp^j} = \gamma^t$, so $\alpha^{p^{2j}-1} = 1$, and consequently $j = n$. Therefore $\gamma^{t(p^n+1)} = 1$, so $(p^n - 1) \mid t$ and thus t is even. Let $\beta = \gamma^{t/2}$. Then

$$f(x) = \prod_{k=0}^{2n-1} \left(x + \beta^{p^k}\right) \cdot \prod_{k=0}^{2n-1} \left(x - \beta^{p^k}\right),$$

and each of these products lies in $\mathbb{F}_p[x]$. □

Acknowledgments

We thank the Heilbronn Institute for Mathematical Research for sponsoring this conference on number theory and polynomials. We also thank Erich Kaltofen for Theorem 6.2. In addition, we thank the center for Interdisciplinary Research in the Mathematical and Computational Sciences (IRMACS) and the High Performance Computing Centre at Simon Fraser University for computational resources.

References

[1] R. H. Barker, *Group synchronizing of binary digital systems*, Communication Theory, Butterworths Sci. Pub., London, 1953, pp. 273–287.
[2] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, Berlin, 1971.
[3] E. Beller and D. J. Newman, *An extremal problem for the geometric mean of polynomials*, Proc. Amer. Math. Soc. **39** (1973), 313–317.
[4] P. Borwein, K.-K. S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than 6.34*, IEEE Trans. Inform. Theory **50** (2004), 3234–3249.
[5] P. Borwein and M. J. Mossinghoff, *A question of irreducibility* (2006), In preparation.
[6] P. Borwein, *Computational Excursions in Analysis and Number Theory*, CMS Books Math./Ouvrages Math. SMC, vol. 10, Springer-Verlag, New York, 2002.
[7] ———, *Paul Erdős and polynomials*, Paul Erdős and His Mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 161–174.
[8] F. W. Carroll, D. Eustice, and T. Figiel, *The minimum modulus of polynomials with coefficients of modulus one*, J. London Math. Soc. (2) **16** (1977), 76–82.
[9] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory Ser. A **55** (1990), 49–59.

[10] S. Eliahou and M. Kervaire, *Barker sequences and difference sets*, Enseign. Math. (2) **38** (1992), 345–382.
[11] ———, *Corrigendum to "Barker sequences and difference sets"*, Enseign. Math. (2) **40** (1994), 109–111.
[12] P. Erdős, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.
[13] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press, Somerset, England, 1996.
[14] G. T. Fielding, *The expected value of the integral around the unit circle of a certain class of polynomials*, Bull. London Math. Soc. **2** (1970), 301–306.
[15] M. L. Fredman, B. Saffari, and B. Smith, *Polynômes réciproques: conjecture d'Erdős en norme L^4, taille des autocorrélations et inexistence des codes de Barker*, C. R. Acad. Sci. Paris Sér. I Math. **308** (1989), 461–464.
[16] M. J. E. Golay, *A class of finite binary sequences with alternate autocorrelation values equal to zero*, IEEE Trans. Inform. Theory **18** (1972), 449–450.
[17] ———, *The merit factor of long low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **28** (1982), 543–549.
[18] J. Jedwab and S. Lloyd, *A note on the nonexistence of Barker sequences*, Des. Codes Cryptogr. **2** (1992), 93–97.
[19] J. Jedwab, *A survey of the merit factor problem for binary sequences*, Sequences and Their Applications—Proceedings of SETA 2004, Lecture Notes in Comput. Sci., vol. 3486, Springer-Verlag, New York, 2005, pp. 30–55.
[20] J.-P. Kahane, *Sur les polynômes à coefficients unimodulaires*, Bull. London Math. Soc. **12** (1980), 321–342.
[21] T. W. Körner, *On a polynomial of Byrnes*, Bull. London Math. Soc. **12** (1980), 219–224.
[22] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), 171–188.
[23] J. E. Littlewood, *On polynomials* $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$, J. London Math. Soc. **41** (1966), 367–376.
[24] ———, *Some Problems in Real and Complex Analysis*, D. C. Heath and Co., Lexington, Mass., 1968.
[25] K. Mahler, *On two extremum properties of polynomials*, Illinois J. Math. **7** (1963), 681–701.
[26] D. J. Newman, *Norms of polynomials*, Amer. Math. Monthly **67** (1960), 778–779.
[27] ———, *An L^1 extremal problem for polynomials*, Proc. Amer. Math. Soc. **16** (1965), 1287–1290.
[28] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859.
[29] B. Saffari, *Barker sequences and Littlewood's "two-sided conjectures" on polynomials with ± 1 coefficients*, Séminaire d'Analyse Harmonique, Année 1989/90, Univ. Paris XI, Orsay, 1990, pp. 139–151.
[30] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), 929–952.
[31] H. S. Shapiro, *Extremal problems for polynomials and power series*, Master's Thesis, Mass. Inst. of Technology, 1951.
[32] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.
[33] R. Turyn, *On Barker codes of even length*, IEEE Trans. Inform. Theory **51** (1963), 1256.
[34] ———, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.
[35] ———, *Sequences with small correlation*, Error Correcting Codes (Proc. Sympos. Math. Res. Center, Madison, Wis.), John Wiley, New York, 1968, pp. 195–228.

Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C. V5A 1S6 Canada
E-mail address: pborwein@cecm.sfu.ca

Department of Mathematics, Davidson College, Davidson, North Carolina 28035-6996, USA
E-mail address: mjm@member.ams.org