RUDIN-SHAPIRO-LIKE POLYNOMIALS IN $L_4$

PETER BORWEIN AND MICHAEL MOSSINGHOFF

Abstract. We examine sequences of polynomials with $\{+1, -1\}$ coefficients constructed using the iterations $p(x) \rightarrow p(x) \pm x^{d+1}p^*(-x)$, where $d$ is the degree of $p$ and $p^*$ is the reciprocal polynomial of $p$. If $p_0 = 1$ these generate the Rudin-Shapiro polynomials. We show that the $L_4$ norm of these polynomials is explicitly computable. We are particularly interested in the case where the iteration produces sequences with smallest possible asymptotic $L_4$ norm (or, equivalently, with largest possible asymptotic merit factor). The Rudin-Shapiro polynomials form one such sequence.

We determine all $p_0$ of degree less than 40 that generate sequences under the iteration with this property. These sequences have asymptotic merit factor 3. The first really distinct example has a $p_0$ of degree 19.

1. Introduction

We are interested in the $L_4$ norm of a polynomial with coefficients $\{+1, -1\}$ (or some other fixed set of coefficients), with the most interesting case being when the norm is small. The norm is the $L_\alpha$ norm on the boundary of the unit disc defined by

$$\|p\|_\alpha = \left( \frac{1}{2\pi} \int_0^{2\pi} |p(e^{i\theta})|^\alpha \, d\theta \right)^{1/\alpha}.$$ 

We call a polynomial with coefficients $\{+1, -1\}$ of degree $n$ a Littlewood polynomial of degree $n$ and denote this class by $\mathcal{L}_n$.

The $L_2$ norm of any element of $\mathcal{L}_{n-1}$ is $\sqrt{n}$, and this is, of course, a lower bound for the $L_4$ norm. There are two natural measures of smallness for the $L_4$ norm of a polynomial $p$ in $\mathcal{L}_{n-1}$. One is the ratio of the $L_4$ norm to the $L_2$ norm, $\|p\|_4/\sqrt{n}$. The other (equivalent) measure is the merit factor, defined by

$$\text{MF}(p) = \frac{\|p\|_2^4}{\|p\|_4^4 - \|p\|_2^4} = \frac{n^2}{\|p\|_4^4 - n^2}.$$ 

The expected $L_4$ norm of an element of $\mathcal{L}_n$ is computed in [25] (see also [3]); the expected merit factor is 1. The $L_4$ norms of the Rudin-Shapiro polynomials are explicitly computed by Littlewood [22] (see also [25]); their merit factors tend to 3. We also compute this in this paper.

In §2 we analyse the Rudin-Shapiro-like polynomials generated by the iterations

$$p(x) \rightarrow p(x) \pm x^{d+1}p^*(-x).$$

Received by the editor April 14, 1998.

1991 Mathematics Subject Classification. Primary 11J54, 11B83, 12-04.

Key words and phrases. Restricted coefficients; $-1, 0, 1$ coefficients; Rudin-Shapiro polynomials; Littlewood conjectures.
We show that the merit factors of the polynomials generated by these iterations with initial polynomial $p_0$ approach

$$\frac{1}{4\gamma/3 - 1},$$

where

$$\gamma = \frac{\|p_0\|^4 + \|p_0(z)p_0(-z)\|^2}{2\|p_0\|^2} \geq 1.$$ 

Note that the maximum possible asymptotic merit factor is 3, and this occurs when $\gamma = 1$. In $\S 3$ we address the problem of determining when $\gamma = 1$, and we find all $p_0$ with this property of degree less than 40.

It is possible to construct sequences with asymptotic merit factor 6. Golay [14] gives a heuristic argument that a sequence of polynomials explored by Turyn has limiting merit factor 6, and this is proved rigorously in [15]. Turyn’s polynomials are constructed by cyclically permuting the coefficients of the Fekete polynomials

$$f_q(z) := \sum_{k=0}^{q-1} \left(\frac{k}{q}\right) z^k$$

by approximately $q/4$. Here, $q$ is a prime number and $\left(\frac{k}{q}\right)$ is the Legendre symbol. The Fekete polynomials themselves have asymptotic merit factor $3/2$, and different amounts of cyclic permutations can give rise to any asymptotic merit factor between $3/2$ and 6.

Golay [14] speculates that 6 may be the largest possible asymptotic merit factor. He writes, “the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors.” Newman and Byrnes [25], apparently independently, make a similar conjecture. Computations by a number of people (including the authors) on polynomials up to degree 200 lead us to believe that higher merit factors are probably possible, and so to doubt these conjectures. See [13], [23], [27], and the web page of A. Reinholz at http://borneo.gmd.de/~andy/ACR.html.

All of these explorations are closely related to Littlewood’s conjecture that it is possible to find polynomials $p_n \in L_{n-1}$, for all $n \geq 1$, satisfying

$$C_1 \sqrt{n} \leq |p_n(z)| \leq C_2 \sqrt{n}$$

for all $z$ with $|z| = 1$, where $C_1$ and $C_2$ are positive absolute constants. See [22]. As a finer form of this problem, replace the constants $C_1$ and $C_2$ by the optimal values $C_1(n)$ and $C_2(n)$ for each $n$. It follows from a related conjecture of Erdős [11] that $C_2(n)$ remains bounded away from 1, independently of $n$. These conjectures are all still open.

The Rudin-Shapiro polynomials (which some argue should be called the Shapiro polynomials) satisfy the upper bound in Littlewood’s conjecture. No sequence is known which satisfies the lower bound.

When $q$ is an odd prime, the Fekete polynomial $f_q(z)$ has modulus $\sqrt{q}$ at each $q$th root of unity (except at $z = 1$, where it vanishes), and one might hope that they also satisfy the upper bound in Littlewood’s conjecture, but Montgomery [24] shows that this is not the case.
2. The iteration

Let \( p^* \) denote the reciprocal polynomial of \( p \): \( p^*(z) = z^d p(1/z) \), where \( d \) is the degree of \( p \). We consider the following construction.

**Iteration 1.** Let \( p_0(z) \) be a polynomial of degree \( D - 1 \) with coefficients in a set \( A \) of complex numbers, and suppose that \( p_0(0) \neq 0 \). Let

\[
p_{n+1}(z) = p_n(z) + z^{d+1} p_n(-z)
\]

where \( d \) is the degree of \( p_n \). Then \( p_n \) is a polynomial of degree \( 2^n D - 1 \) with all coefficients in \( A \cup -A \). Furthermore, if

\[
R_n := p_n(z) \quad \text{and} \quad S_n := p^*_n(-z),
\]

then

\[
R_{n+1} = R_n + z^{d+1} S_n
\]

and

\[
S_{n+1} = (-1)^d (R_n - z^{d+1} S_n).
\]

**Proof.** Most of this is simple calculation. Observe that

\[
p_{n+1}(z) = p_n(z) + (-1)^d z^{2d+1} p_n(-1/z),
\]

so

\[
p_{n+1}(-1/z) = p_n(-1/z) - (-1)^d z^{-2d-1} p_n(z),
\]

and multiplying this equation by \(-z^{2d+1}\) yields the second form of the iteration.

**Lemma 1.** In the notation of Iteration 1,

\[
|R_n(z)|^2 + |S_n(z)|^2 = 2^n (|p_0(z)|^2 + |p^*_0(-z)|^2),
\]

provided \(|z| = 1\). Furthermore,

\[
\frac{|R_n(z)|^2}{\|R_n\|^2} + \frac{|S_n(z)|^2}{\|S_n\|^2} = \frac{|p_0(z)|^2}{\|p_0\|^2} + \frac{|p^*_0(-z)|^2}{\|p^*_0\|^2}.
\]

**Proof.** The first statement follows from the parallelogram law for complex numbers:

\[
|R_{n+1}(z)|^2 + |S_{n+1}(z)|^2 = |R_n(z) + z^{d+1} S_n(z)|^2 + |R_n(z) - z^{d+1} S_n(z)|^2
\]

\[
= 2(|R_n(z)|^2 + |S_n(z)|^2).
\]

The second statement follows on observing that \( \|R_{n+1}\|_2^2 = 2 \|R_n\|_2^2 \) and \( \|S_{n+1}\|_2^2 = 2 \|S_n\|_2^2 \).

We wish to compute the \( L_4 \) norm of \( p_n \). For this we follow Littlewood [22].

**Theorem 1.** In the notation of Iteration 1, let \( y_n = \|p_n\|_4/\|p_n\|_2 \) for \( n \geq 0 \), and let

\[
\gamma = \frac{\|p_0\|_4^4 + \|p_0(z)p^*_0(-z)\|_2^2}{2 \|p_0\|_2^2}.
\]

Then

\[
y_n = \frac{4\gamma}{3} + \left(y_0 - \frac{4\gamma}{3}\right) \left(-\frac{1}{2}\right)^n.
\]
Proof. With $R_n$ and $S_n$ as in Iteration 1, let

$$x_n := \|R_n\|_4^4 = \|S_n\|_4^4$$

and

$$w_n := \|R_nS_n\|_2^2.$$

Then, with $z = e^{i\theta}$ and $d = \deg(R_n)$,

$$2x_{n+1} = \|R_{n+1}\|_4^4 + \|S_{n+1}\|_4^4$$

$$= \frac{1}{2\pi} \int_{0}^{2\pi} \left( |R_n(z) + z^{d+1}S_n(z)|^4 + |R_n(z) - z^{d+1}S_n(z)|^4 \right) d\theta.$$

If we use the identity for complex numbers

$$|u + v|^4 + |u - v|^4 = 2(|u|^4 + |v|^4) + 4\Re(u\overline{v})^2 + 8|uv|^2$$

with $u := z^{d+1}S_n(z)$ and $v := R_n(z)$, we deduce that

$$2x_{n+1} = 4x_n + 8w_n + \frac{4}{2\pi} \int_{0}^{2\pi} \Re(R_n(z)\overline{z^{d+1}S_n(z)})^2 d\theta.$$

Now $R_n(z)\overline{z^{d+1}S_n(z)} = R_n^*(1/z)S_n(1/z)/z$, a polynomial in $1/z$ with constant term 0, so the integral above is 0. Thus

(1) $$x_{n+1} = 2x_n + 4w_n.$$  

We now observe that, with Lemma 1,

$$2x_n + 2w_n = \frac{1}{2\pi} \int_{0}^{2\pi} \left( |R_n(z)|^2 + |S_n(z)|^2 \right)^2 d\theta$$

$$= \frac{2^{2n}}{2\pi} \int_{0}^{2\pi} \left( |p_0(z)|^2 + |p_0^*(-z)|^2 \right)^2 d\theta$$

$$= \frac{2^{2n+2}}{2\pi} \int_{0}^{2\pi} \left( |p_0(z)|^4 + |p_0(z)p_0^*(-z)|^2 \right) d\theta$$

$$= 2^{2n+2} \left( \|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2 \right).$$

From this and (1) we deduce that

$$x_{n+1} = -2x_n + 2^{2n+3} \left( \|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|_2^2 \right).$$

Since $\|p_{n+1}\|_2^2 = 4\|p_n\|_2^4$, this yields

$$y_{n+1} = -\frac{y_n}{2} + 2\gamma,$$

which simply solves to give the result. 

An immediate consequence of this is the following.
Corollary 1. The sequence \( p_n(z) \) generated by Iteration 1 satisfies
\[
\lim_{n \to \infty} \frac{\|p_n\|_4}{\|p_n\|_2} = \left( \frac{4\gamma}{3} \right)^{1/4}
\]
and
\[
\lim_{n \to \infty} \text{MF}(p_n) = \frac{1}{4\gamma/3 - 1},
\]
where
\[
\gamma = \frac{\|p_0\|_4^4 + \|p_0(z)p_0^*(-z)\|^2}{2\|p_0\|_2^4} \geq 1.
\]

Proof. The only part needing proof is that \( \gamma \geq 1 \). For this, note that
\[
\|p\|_4^4 + \|p(z)p^*(-z)\|^2 = \frac{2}{2\pi} \int_0^{2\pi} \left( \frac{|p(z)|^2 + |p^*(-z)|^2}{2} \right)^2 d\theta
\]
\[
\geq \frac{2}{2\pi} \int_0^{2\pi} \frac{|p(z)|^2 + |p^*(-z)|^2}{2} \right)^2 d\theta
\]
\[
= 2\|p\|_2^4.
\]
Here we have used the fact that \( L_2(q) \geq L_1(q) \).

It is easy to check that the same results hold for the iteration \( p_{n+1}(x) = p_n(x) - x^{d+1}p_n^*(-x) \).

Define
\[
\gamma(p) = \frac{\|p\|_4^4 + \|p(x)p^*(-x)\|^2}{2\|p\|_2^4}
\]
and let
\[
T_{\pm}(p) = p(x) \pm x^{d+1}p^*(-x).
\]

A direct computation, as in the proof of Theorem 1, shows that \( \gamma(T_{\pm}(p)) = \gamma(p) \).

Thus, by an obvious analogue of Corollary 1, if \( \{q_n\} \) is a sequence of polynomials generated by \( q_{n+1} = T_{\pm}(q_n) \) for some choice of signs, then
\[
\lim_{n \to \infty} \frac{\|q_n\|_4}{\|q_n\|_2} = \left( \frac{4\gamma(q_0)}{3} \right)^{1/4}.
\]

We remark that the usual Rudin-Shapiro polynomials satisfy the recurrence
\[
P_{n+1}(x) = P_n(x) - (-1)^n x^{2^n} P_n^*(-x)
\]
and
\[
Q_{n+1}(x) = P_n(x) + (-1)^n x^{2^n} P_n^*(-x)
\]
for \( n \geq 1 \), so
\[
\{P_{n+1}, Q_{n+1}\} = \{T_{+}(P_n), T_{-}(P_n)\}.
\]

The interesting question now becomes: For which \( p \) is \( \gamma(p) = 1? \)
3. Littlewood Polynomials with $\gamma = 1$

Polynomials which satisfy $\gamma(p) = 1$ are of special interest in that they give rise to sequences of polynomials (under iteration by $T_\pm$) that satisfy

$$\lim_{n \to \infty} \frac{\|p_n\|_4}{\|p_n\|_2} = \left(\frac{4}{3}\right)^{1/4},$$

the smallest possible limit under the process. The interesting observation is that many such $p$ exist. Indeed, there are 128 distinct such $p$ of degree 19, which we list later in this section. One example is

$$1 + x - x^2 + x^3 + x^4 + x^5 - x^6 + x^7 - x^8 + x^9 - x^{10} - x^{11}
+ x^{12} + x^{13} + x^{14} - x^{15} - x^{16} - x^{17} - x^{18} + x^{19}.$$  

We describe an algorithm for determining all Littlewood polynomials $p$ of degree $d$ having $\gamma(p) = 1$. We first require some preliminary lemmas.

**Lemma 2.** Let $p(x) = \sum_{k=0}^{d} x^k$. Then $\|p\|_4^4 = (d + 1)(2d^2 + 4d + 3)/3$ and $\|p(x)p^*(-x)\|_2^2 = d + 1$.

**Proof.** Since $p(x)^2 = (d + 1)x^d + \sum_{k=0}^{d-1}(k + 1)(x^k + x^{2d-k})$, the first identity follows easily from Parseval’s formula. For the second identity, we have

$$p(x)p^*(-x) = \frac{x^{d+1} - 1}{x - 1} \cdot \frac{x^{d+1} + (-1)^d}{x + 1}$$

$$= \begin{cases} 
\sum_{k=0}^{d} x^{2k}, & d \text{ even,} \\
(x^{d+1} - 1) \sum_{k=0}^{(d-1)/2} x^{2k}, & d \text{ odd,}
\end{cases}$$

and the formula follows. $\square$

**Lemma 3.** Let $p$ be a Littlewood polynomial of degree $d$. The coefficient of $x^d$ in $p(x)p^*(-x)$ is 0 if $d$ is odd and 1 if $d$ is even.

**Proof.** Write $p(x) = \sum_{k=0}^{d} a_k x^k$, so that $p^*(-x) = (-1)^d \sum_{k=0}^{d} a_{d-k}(-1)^k x^k$. The coefficient of $x^d$ in the product is therefore

$$(-1)^d \sum_{i+j=d} a_i a_{d-j}(-1)^j = \sum_{i=0}^{d} (-1)^i a_i^2 = \sum_{i=0}^{d} (-1)^i,$$

and the result follows. $\square$

**Lemma 4.** Suppose $p$ and $q$ are Littlewood polynomials of degree $d$. Then $\|p\|_4^4 \equiv \|q\|_4^4$ (mod 8), and $\|p(x)p^*(-x)\|_2^2 \equiv \|q(x)q^*(-x)\|_2^2$ (mod 8).

**Proof.** Let $p(x) = \sum_{k=0}^{d} a_k x^k$ and $p(x)^2 = \sum_{k=0}^{2d} b_k x^k$. It is enough to prove the statement for the case where $p$ and $q$ are identical except for one coefficient, so assume that $q(x) = p(x) - 2a_m x^m$ for some $m$. Write $q(x)^2 = \sum_{k=0}^{2d} \beta_k x^k$. Then

$$\beta_k = \begin{cases} 
b_k - 4a_m a_{k-m}, & m \leq k \leq m + d, \ k \neq 2m, \\
b_k, & \text{otherwise.}
\end{cases}$$

Therefore

$$\|q\|_4^4 = \|p\|_4^4 + 16d - 8a_m \sum_{m \leq k \leq m + d} a_{k-m} b_k$$

(2)
and the first assertion of the theorem follows. For the second, let
\[ p(x)p^*(-x) = \sum_{k=0}^{2d} c_k x^k \quad \text{and} \quad q(x)q^*(-x) = \sum_{k=0}^{2d} \delta_k x^k. \]

Now
\[ q(x)q^*(-x) = (p(x) - 2a_m x^m) (p^*(-x) - 2a_m (-1)^m x^{d-m}), \]
so \( \delta_k^2 \equiv c_k^2 \pmod{4} \) for each \( k \). Because \( \delta_d = c_d \) by Lemma 3 and \( \delta_k = \pm \delta_{2d-k} \), it follows that \( \|p(x)p^*(-x)\|_2^2 \equiv \|q(x)q^*(-x)\|_2^2 \pmod{8}. \)

We immediately deduce the following theorem.

**Theorem 2.** If \( p \) is a Littlewood polynomial of degree \( d \) and \( d \equiv 2 \pmod{4} \), then \( \gamma(p) > 1 \).

**Proof.** By Lemmas 2 and 4, we have \( \|p\|_4^2 + \|p(x)p^*(-x)\|_2^2 \equiv 6 \pmod{8} \), but \( 2\|p\|_2^2 \equiv 2 \pmod{8} \), so \( \gamma(p) \neq 1 \). The result follows from Corollary 1. \( \square \)

In searching for Littlewood polynomials \( p \) having \( \gamma(p) = 1 \), clearly we may assume that the coefficients of the two highest-order terms are both 1. We employ a Gray code \( \{2\} \) to enumerate all possible combinations of signs among the lower-order terms. This way, each polynomial considered differs in exactly one position from the previous polynomial tested, and we may use formulas (2) and (3) to compute each \( \gamma \) in \( O(d) \) time.

**Algorithm 1.** Rudin-Shapiro like polynomials in \( L_4 \).

**Input.** \( d \), a positive integer, \( d \not\equiv 2 \pmod{4} \).

**Output.** All Littlewood polynomials \( p(x) \) of degree \( d \) having \( \gamma(p) = 1 \).

**Data.** \( a_k \) is the coefficient of \( x^k \) in \( p(x) \), \( b_k \) in \( p(x)^2 \), and \( c_k \) in \( p(x)p^*(-x) \).

**Initialize.** Set the \( a_k, b_k, \) and \( c_k \) for the polynomial \( p(x) = \sum_{k=0}^{d} x^k \). Set \( v_k = 0 \) for \( 1 \leq k < d \). Choose \( s, t, s_0, \) and \( t_0 \) so that \( (d+1)(2d^2 + 4d + 3)/3 = 8s + s_0 \), \( d+1 = 8t + t_0 \), \( 0 \leq s_0 < 8 \), and \( 0 \leq t_0 < 8 \). Let \( u = (2(d+1)^2 - s_0 - t_0)/8 \).

**Loop.** Enumerate all possible combinations of signs among the lower order \( d-1 \) coefficients of the polynomial using a Gray code. Execute the following statements when changing the sign of the \( m \)th coefficient of the polynomial.

\[
\begin{align*}
s &\leftarrow s + 2d - a_m \sum_{0 \leq k \leq d} a_k b_{k+m} \\
& \text{for } k \neq m \\\nb_k &\leftarrow b_k - 4a_m a_{k-m}, \quad m \leq k \leq d + m, \quad k \neq 2m \\
v_k &\leftarrow (-1)^{d+m-k+1} a_m a_{m+k-d}, \quad m \leq k < d \\
v_k &\leftarrow v_k + (-1)^{m+1} a_m a_{m+k-d}, \quad d - m \leq k < d \\
t &\leftarrow t + \sum_{k=1}^{d} v_k (c_k + v_k) \\
c_k &\leftarrow c_k + 2v_k, \quad 1 \leq k < d \\
v_k &\leftarrow 0, \quad 1 \leq k < d \\
a_m &\leftarrow -a_m \\
\text{If } s + t = u \text{ then print } p(x).
\end{align*}
\]

Searching through degree 39, we find many polynomials with \( \gamma = 1 \) at the degrees of the Rudin-Shapiro polynomials, plus a number of examples of degree
Theorem 3. Let $z$ be a polynomial, and define $U(p) = xp(x^2) + p^*(-x^2)$. Then $\gamma(U(p)) = \gamma(p)$.

Proof. Let $q = U(p)$. Then
\[
\|q\|_4^4 = \|(xp(x^2) + p^*(-x^2))\|_2^2 \\
= \|x^2 p(x^2)^2 + p^*(-x^2)^2\|_2^2 + 2\|xp(x^2) p^*(-x^2)\|_2^2 \\
= \|xp(x^2)^2 + p^*(-x^2)^2\|_2^2 + 4\|p(x)p^*(-x)\|_2^2.
\]

The first term is
\[
\frac{1}{2\pi} \int_0^{2\pi} |zp(z)^2 + p^*(-z)^2|^2 d\theta = 2\|p\|_4^4 + 4\int_0^{2\pi} \text{Re}(z^{1-2\text{deg}(p)} p(z)^2 p(-z)^2) d\theta
\]
with $z = e^{i\theta}$, and the integral is 0 because $p(x)p(-x)$ is an even function. Thus
\[
\|q\|_4^4 = 2\|p\|_4^4 + 4\|p(x)p^*(-x)\|_2^2.
\]
Next, we compute
\[\|q(x)q^*(-x)\|_2^2 = \|p^*(-x^2) + xp(x^2)(p^*(x^2) - xp(-x^2))\|_2^2 = \|p^*(x^2)p^*(-x^2) - x^2p(x^2)p(-x^2)\|_2^2 + \|x(p(x^2)p^*(x^2) - p(-x^2)p^*(-x^2))\|_2^2 = \|p^*(x)p^*(-x) - xp(x)p(-x)\|_2^2\|p(x)p^*(x) - p(-x)p^*(-x)\|_2^2.
\]
The first term equals 2\|p(x)p(-x)\|_2^2 because \(p(x)p(-x)\) is an even function. The second term is
\[
\frac{1}{2\pi} \int_0^{2\pi} |p(z)|^2 - |p(-z)|^2|^2 \, d\theta = 2\|p\|_4^4 - 2\|p(x)p(-x)\|_2^2,
\]
so
\[
(5) \quad \|q(x)q^*(-x)\|_2^2 = 2\|p\|_2^4.
\]
Clearly, \(\|q\|_2^2 = 2\|p\|_2^2\), and this fact combined with (4) and (5) proves the theorem.

Thus, the four operators \(T_+, T_-, U,\) and \(U^*\) (the reciprocal of \(U, U^*(p) = xp(-x^2) + p^*(x^2)\)) in general allow us to construct four polynomials of degree \(2d + 1\) with \(\gamma = 1\) for each polynomial of degree \(d\) with this property.

ACKNOWLEDGMENT

We thank the referee for several valuable suggestions.

REFERENCES

21. J. E. Littlewood, *On polynomials $\sum^n \pm z^m$ and $\sum^m e^{n|m|z^m}$, $z = e^{bi}$*, J. London Math. Soc. 41 (1966), 367–376. [MR 33:1237]