Search for ultraflat polynomials with plus and minus one coefficients

Andrew Odlyzko

School of Mathematics
University of Minnesota
Minneapolis, MN 55455, USA
odlyzko@umn.edu
http://www.dtc.umn.edu/∼odlyzko
Revised version, May 18, 2017

Dedicated to Ron Graham on his 80th birthday

Abstract. It is not known whether there exist polynomials with plus and minus one coefficients that are almost constant on the unit circle (called ultraflat). Extensive computations described in this paper strongly suggest such polynomials do not exist, and lead to conjectures about the precise degree to which flatness can be approached according to various criteria. The evidence shows surprisingly rapid convergence to limiting behavior. Connections to problems about the Golay merit factor, Barker sequences, Golay-Rudin-Shapiro polynomials, and others are discussed. Some results are presented on extensions where the coefficients are allowed to be roots of unity of orders larger than two. It is pointed out that one conjecture of Littlewood about polynomials with plus and minus one coefficients is true, while another is very likely to be false, as it is inconsistent with another Littlewood conjecture that is supported by the data.

1 Introduction

There are many very appealing and easy to state problems about the behavior of polynomials with restricted coefficients that have proved very hard. One that was raised in pure mathematics context by Erdős [11] and later extended and popularized by Littlewood in several of his papers, such as [22], and in his book [23], concerns the degree to which the absolute value of a polynomial can be almost constant when the argument runs over the unit circle. This problem also arose in several engineering problems, cf. [32,35]. If the coefficients are not constrained, this is of course trivial. But what if the coefficients are all forced to be of absolute value 1, or, even more restrictively, equal ± 1?

We define

$$\mathbb{U}_n = \{F(z) = \sum_{k=0}^{n} a_k z^k,\ a_k = \pm 1\} \tag{1}$$

and similarly $\mathbb{V}_n$ where we allow $a_k \in \mathbf{C}, |a_k| = 1$. A simple computation (trivial case of Parseval's identity) shows that for $F(z) \in \mathbb{V}_n$ (and therefore also for $F(z) \in \mathbb{U}_n$),

$$\|F\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi} |F(e^{i\theta})|^2 d\theta = \frac{1}{2\pi}\sum_{j,k=0}^{n}\int_0^{2\pi} a_j\bar{a}_k e^{i(j-k)\theta}d\theta = \sum_{k=0}^{n}|a_k|^2 = n+1. \qquad (2)$$

Hence if $F(z) \in \mathbb{V}_n$ is ultraflat, its absolute value must be close to $\sqrt{n+1}$. This motivates the definition, for $F(z) \in \mathbb{V}_n$,

$$M(F) = \max_{|z|=1}\frac{|F(z)|}{\sqrt{n+1}}, \qquad m(F) = \min_{|z|=1}\frac{|F(z)|}{\sqrt{n+1}}, \qquad W(F) = M(F) - m(F). \qquad (3)$$

All graphs in this paper are of (Re($F(e^{i\theta})$, Im($F(e^{i\theta})$)$/\sqrt{n+1}$ for $0 \le \theta \le 2\pi$ to obtain comparisons that are independent of the degree of $F(z)$.

$W(F)$ is the minimal width of an annulus centered at the origin that contains the graph of $F(z)/\sqrt{n+1}$. Ultraflat polynomials $F(z)$ of high degree would have $M(F) \approx m(F) \approx 1$ and $W(F) \approx 0$.

For random $F(z)$ taken from $\mathbb{V}_n$ or $\mathbb{U}_n$,

$$M(F) \sim \sqrt{\log n} \qquad (4)$$

as $n \to \infty$ with probability tending to 1. An upper bound of this form was obtained by Salem and Zygmund, and the asymptotic form for a special case by Halasz [17] and in the general form by Gersho et al. [13]. (The last result allows for the a_k to be drawn from very general distributions, with the main requirement being that the a_k be independent. The a_k do not even have to be identically distributed. That paper also shows that for most $F(z)$, large values are taken on in at least $\log n$ regions.) By similar methods one can show that $m(F) \to 0$ for most $F(z)$. Thus ultraflat polynomials in either $\mathbb{U}_n$ or $\mathbb{V}_n$, if they exist, are relatively rare, which proves the first part of Littlewood's conjecture (C_3), [23], p. 29. However, the second part of that conjecture, which predicts the number of such polynomials is extremely small, namely $O(n^3)$, is almost surely false. If, for a large n, there exists even one polynomial with $M(F)$ bounded above, and $m(F)$ bounded away from zero (in both cases with bounds independent of n), as is predicted by Littlewood's conjecture (C_1), and as is strongly suggested by the results of this paper, then Section 3 shows there have to be many such.

For a long time the prevailing opinion seemed to be that there were no ultraflat polynomials in $\mathbb{V}_n$. It came as a surprise to many, therefore, when in 1980 Kahane [19], building on earlier work of Körner [20] and other investigators, showed this was not correct, and that for any $\epsilon > 0$, for sufficiently large n there are $F(z) \in \mathbb{V}_n$ with $W(F) < \epsilon$. Kahane's method is not constructive, as it uses a randomization procedure to guarantee that $|a_k| = 1$. Kahane's construction was recently improved by Bombieri and Bourgain [2], who obtained smaller error terms, and, even more important, obtained explicit constructions, thus eliminating the non-constructive element.

This paper investigates the problem that the Kahane and also the Bombieri and Bourgain papers left open, namely what happens if we insist the coefficients be ± 1. Let

$$M_n = \min_{F \in \mathbb{U}_n} M(F), \qquad (5)$$

$$m_n = \max_{F \in \mathbb{U}_n} \; m(F), \tag{6}$$

$$W_n = \min_{F \in \mathbb{U}_n} \; W(F). \tag{7}$$

Very little is known theoretically, although some very recent work [9] that is yet to be verified claims to prove that ultraflat polynomials do not exist in $\mathbb{U}_n$.

For $n = 2^k - 1$, it is known that $M_n \leq \sqrt{2}$, since the Golay-Rudin-Shapiro (GRS) polynomials achieve this bound, cf. [3]. These polynomials are usually referred to in the literature as the Rudin-Shapiro polynomials [30,33]. However, they were discovered independently by Golay [14], so it is appropriate to attach his name to them. For references to some of the large literature on these remarkable polynomials, see, for example [3,6]. It can be shown, using GRS polynomials, that M_n is bounded as n ranges over all positive integers. But that is just about all that is known rigorously. On the lower side, it is not even known whether $\limsup_{n\to\infty} m_n > 0$. (See Section 5.)

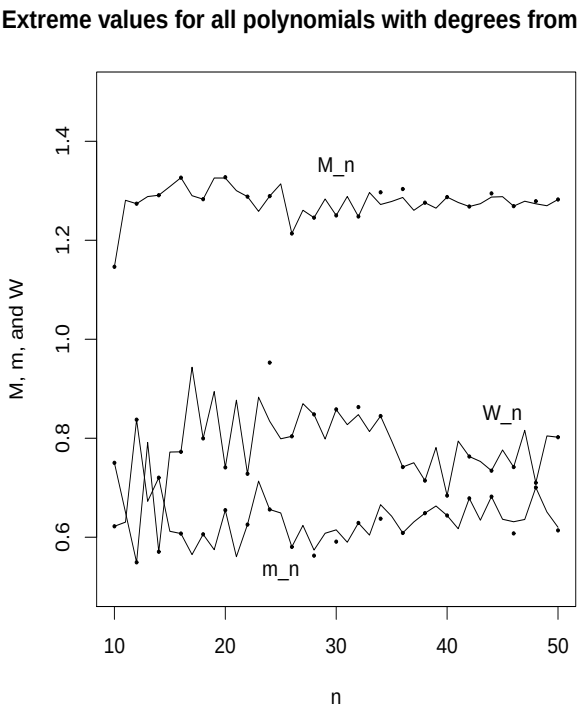

Fig. 1. Values of M_n, m_n and W_n for $10 \leq n \leq 50$. Scatter plot gives values of M_n^*, m_n^*, and W_n^* for even n in that range.

This paper is based on exhaustive computational searches for extremal polynomials in $\mathbb{U}_n$. The first part examined all $F(z) \in \mathbb{U}_n$ for $n \leq 52$. These computations extend unpublished computations of the author in the late 1980s and smaller scale searches of Robinson [28]. These searches lead to the conjecture that each of the following limits

exists:

$$\lim_{n\to\infty} M_n = M, \tag{8}$$

$$\lim_{n\to\infty} m_n = m, \tag{9}$$

$$\lim_{n\to\infty} W_n = W. \tag{10}$$

The computations reported here suggest that $M \approx 1.27, m \approx 0.64$, and $W \approx 0.79$. These conjectures imply that ultraflat polynomials in $\mathbb{U}_n$ do not exist, but that GRS polynomials are far from optimal in terms of never being large. The conjecture that W exists and that $W < 1$ implies there exist constants $0 < c_1 < c_2$ so that for all high degrees N there are polynomials $F(z) \in \mathbb{U}_n$ with $c_1 < m(F) < M(F) < c_2$, which is Littlewood's conjecture (C_1), [23], p. 29.

Fig. 1 shows a graph of the values of M_n, m_n, and W_n for $10 \le n \le 50$. The numerical values for all $n \le 52$ and the polynomials that achieve them (as well as a large collection of other polynomials that come close to the record values) are available on the author's home page. Perhaps some patterns will be found in their coefficients that will help in explicit constructions of high degree polynomials that are close to ultraflat.

It should be noted that the optimal polynomials are not isolated, as in most cases there are many others that have similar values, see Section 3.

Fig. 1 shows M_n converging rapidly, and m_n and W_n considerably more slowly. However, given the low degrees involved, even the rate of convergence for m_n and W_n is rather remarkable, see Section 3.

The dots in Fig. 1 represent the optimal values when we restrict consideration to the very important class of skew-symmetric polynomials. When $F(z) \in \mathbb{U}_n$, $M(F)$ and $m(F)$ are the same for $F(z)$ and for

$$z^n F(\frac{1}{z}), \qquad -F(z), \qquad F(-z). \tag{11}$$

Therefore $F(z) \in \mathbb{U}_n$ can be grouped naturally into octuplets, which makes the search easier. Sometimes these octuplets collapse. The symmetric case, $F(z) = z^n F(\frac{1}{z})$, leads to very poor results for our problem. (This is easily observed with even low-degree polynomials, and there are some rigorous results that show, for example, that symmetric polynomials cannot be ultraflat. For the latest in this area, see [10].) However, when n is even, we usually obtain excellent outcomes from the skew-symmetric polynomials, namely those with

$$F(z) = \pm z^n F(\frac{-1}{z})$$

(where the sign has to be $(-1)^{n/2}$). Those, as was first noticed by Golay in a slightly different context, see Section 2, contain the optimal polynomials in a majority of known cases. This is visible in Fig. 1 when the dot is right on the line. Even when a non-skew-symmetric polynomial is better than any skew-symmetric ones, visible in Fig. 1 when the dot is not right on the corresponding curve, the difference is usually slight. The largest exception to this claim that has been found so far is for W_{24}, which stands out in Fig. 1,

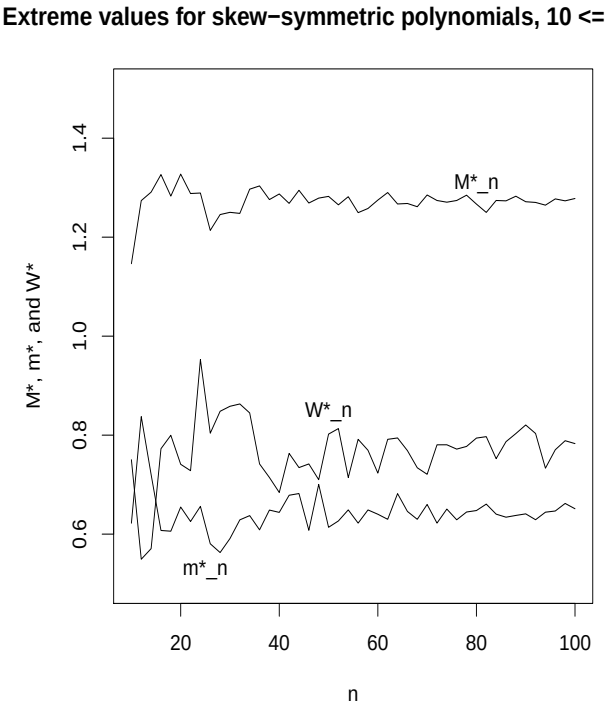

Fig. 2. Values of M_n^*, m_n^*, and W_n^* for even n, $10 \le n \le 100$.

with $W_{24} = 0.8344$, whereas the best result obtainable from skew-symmetric polynomials requires an annulus of width 0.9528.

Fig. 1 naturally suggests the conjecture that if we define M_n^*, m_n^*, and W_n^* in analogy to M_n, m_n, and W_n, but limiting consideration to skew-symmetric polynomials of degree n, then

$$\lim_{\substack{n\to\infty \\ n \text{ even}}} M_n^* = \lim_{n\to\infty} M_n = M,$$
$$\lim_{\substack{n\to\infty \\ n \text{ even}}} m_n^* = \lim_{n\to\infty} m_n = m,$$
$$\lim_{\substack{n\to\infty \\ n \text{ even}}} W_n^* = \lim_{n\to\infty} W_n = W.$$

Since skew-symmetric polynomials have only $n/2+1$ free coefficients, as opposed to $n+1$ for general ones, searches can be carried out about twice as far, and so far have been taken up to $n = 104$. The results for $10 \le n \le 100$ are shown in Fig. 2, and the numerical values for all even $n \le 104$ are in the online tables, together with the corresponding polynomials, and nearly-optimal polynomials. As with general $F(z) \in \mathbb{U}_n$, convergence is fastest for M_n^*, but now m_n^* also appears to converge rapidly, and it is only W_n^* that oscillates to a substantial extent.

The conjectured values for the limits, $M \approx 1.27, m \approx 0.64$, and $W \approx 0.79$ were derived from the computed values of M_n^*, m_n^*, and W_n^*.

2 Golay merit factor and Barker polynomials

Ultraflat polynomials have close connections to the much larger field of discrete sequences and their correlation properties. (For some general information and references, see, for example, the book [3]. For much more detail and extensive references, including numerous applications, see [12,16].) Here we just cite some of the basic results about the Golay merit factor and Barker polynomials. Much more can be found in the references just cited, as well as on the Web pages of the Centre for Experimental and Constructive Mathematics at Simon Fraser University, and the home pages for Michael Mossinghoff and Tamás Erdélyi, for example.

For $a_0, \ldots, a_n = \pm 1$, and $0 \le k \le n$, let

$$c_k = \sum_{j=0}^{n-k} a_j a_{j+k}, \tag{12}$$

and for $k < 0$ let $c_k = c_{-k}$. A Barker sequence $a_0, \ldots, a_n$ is defined by the property that the non-trivial c_k are as small as possible, namely $c_k = 0, \pm 1$ for $1 \le k \le n$. The only nontrivial Barker sequences that are known have $n = 2, 3, 4, 6, 10$, and 12, and are of great utility in communications and radar applications. It is conjectured that there are no more, and it is known [21] that there are no other ones with lengths $n < 4 \cdot 10^{33}$.

To any sequence $a_0, \ldots, a_n = \pm 1$ we can associate the polynomial $F(z) \in \mathbb{U}_n$ with the a_k as coefficients. For this sequence and its polynomial, we define the Golay merit factor

$$G(F) = \frac{(n+1)^2}{2\sum_{k=1}^{n} c_k^2}. \tag{13}$$

A Barker sequence has the denominator $\sim n$, and so $G(F) \sim n$. The largest known $G(F)$ comes from the Barker sequence with $n = 12$, and equals $169/12 = 14.08\ldots$. It is conjectured that this is the largest merit factor among all sequences of all lengths. The second largest is 12.1, coming from the Barker sequence with $n = 10$, and no other merit factors exceeding 10 are known. Golay's conjecture [15] that the highest merit factors should approach 12.32 asymptotically is generally not accepted as likely to be correct. For the latest computations of highest merit factors for all sequences with $n \le 65$ and all skew-symmetric sequences with $n \le 116$, see [26].

If merit factors are bounded, then the c_k are in absolute value on the order of $\sqrt{n}$ on average. That is what random choices of a_k produces.

If the a_k are chosen at random, then for large n, for most sequences $G(F) \sim 1$. GRS polynomials have $G(F) \sim 3$, and the best currently known constructions give $G(F) \sim 6.34$ for large n [18]. However, exhaustive computations for lengths up to 60, and heuristic searches for greater n, frequently find sequences with $G(F) > 9$.

Getting back to polynomials, if $F(z) \in \mathbb{U}_n$, $F(z) = \sum_{k=0}^{n} a_k z^k$, then (all on $|z| = 1$)

$$F(z)\bar{F}(z) = F(z)F(\frac{1}{z}) = \sum_{k=-n}^{n} c_k z^k,$$

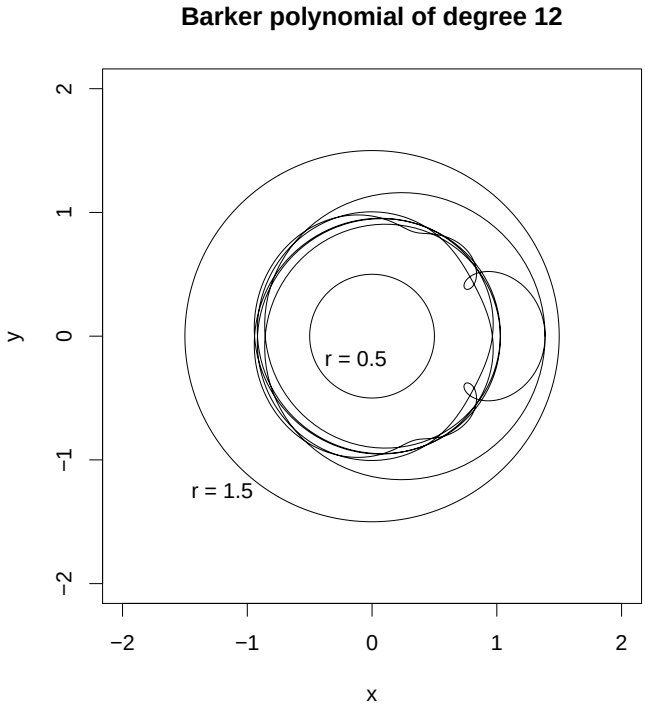

Fig. 3. Real and imaginary parts of the Barker polynomial of degree 12 (scaled by $\sqrt{13}$) as the argument runs over the unit circle, and circles of radii 0.5 and 1.5.

so

$$\|F(z)\|_4^4 = \|F(z)F(\frac{1}{z})\|_2^2 = \sum_{k=-n}^{n} c_k^2.$$

Hence

$$G(F) = \frac{c_0^2}{\sum_{k\neq 0} c_k^2} = \frac{(n+1)^2}{\|F\|_4^4 - \|F\|_2^4}. \tag{14}$$

Ultraflat polynomials $F(z)$ would have $\|F\|_4 \sim \|F\|_2 \sim (1+o(1))\sqrt{n+1}$ and so would give $G(F) \to \infty$. The conjecture that $G(F)$ is bounded therefore implies there are no ultraflat polynomials of high degrees. (For more on connections between sequences and flat polynomials, see also [3,4].)

Eq. (14) shows that there is a relation between high merit factors and flatness. In some cases, the correspondence is very close. The Barker polynomial of degree 10 has the smallest $M(F)$ (= 1.1464) of all polynomials that have been tested, and the Barker polynomial of degree 12 (whose behavior on the unit circle is displayed in Fig. 3) has the largest $m(F)$ (= 0.8375) and the smallest $W(F)$ (= 0.5493) that have been found.

The correlation between high Golay merit factors and flatness is not perfect, as can be seen by the example of the skew-symmetric polynomials of degree 102. Fig. 4 shows the behavior on the unit circle of the polynomial in this set which has the smallest $M(F)$

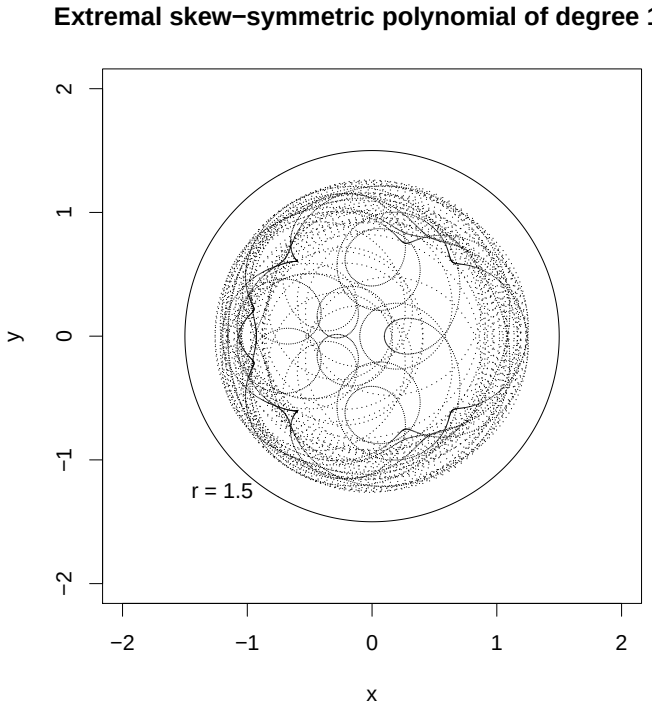

Fig. 4. Real and imaginary parts of the skew-symmetric polynomial of degree 102 which achieves $M(F) = M^*_{102} = 1.2633...$, at 10,000 uniformly spread points over the unit circle, scaled by $\sqrt{103}$, and a circle of radius 1.5.

(= 1.2633) among all skew-symmetric polynomials of degrees $84 \le n \le 104$. It has $G(F) = 5.7973$ (and $m(F) = 0.0985$). However, there is a skew-symmetric polynomial $F(z)$ of degree 102 which achieves $G(F) = 9.5577$ (the highest value that has been found in searches just for high merit factors among skew-symmetric sequences of that length), but it has $M(F) = 1.3689$, $m(F) = 0.5667$. This polynomial does not produce the best values for either $m(F)$ or $W(F)$ for degree 102.

3 Lack of isolation of extreme flat polynomials

In searches for high merit factors, it has been noted that for a given length, the sequence with the highest merit factor is usually not just unique (aside from the obvious symmetries given by (11)), but is isolated, in that the second largest merit factor is considerably smaller. For example, in the searches for flat skew-symmetric polynomials of degree 102 of this paper, the highest merit factor found was 9.5577, and the second highest was only 8.1482. In contrast, the best values of $M(F)$ are usually just a little smaller than second best. As as example, $M^*_{102} = 1.2633$, but aside from the polynomial shown in Fig. 4 that achieves this value and the other three polynomials in its symmetry class, there is another skew-symmetric polynomial that has $M(F) = 1.2647$, and the 10-th smallest value of $M(F)$ is 1.2876. Similar observations hold for the extremal values of $m(F)$ and $W(F)$.

For very large values of the degree n the existence of many polynomials with values of $M(F)$ close to M_n is easy to show (and similarly for m_n and W_n). Since changing one coefficient in $F(z)$ from $+1$ to -1 or vice versa changes the values of $F(z)$ on the unit circle by at most 2, and $M(F)$ scales the maximal value by dividing by $\sqrt{n+1}$, perturbing a bounded number of coefficients of $F(z)$ does not affect $M(F)$ to a perceptible degree. In fact, much more substantial perturbations leave $M(F)$ almost constant for large degrees. If we have a polynomial $F_1(z) \in \mathbb{U}_n$ and we take a random polynomial $F_2(z) \in \mathbb{U}_m$, then, by (4),

$$M(F_1 + z^n F_2) \le M(F_1) + 2\sqrt{\log m}\sqrt{m/n} \tag{15}$$

for most choices of $F_2(z)$. Hence if $m = o(n/(\log n))$ as $n \to \infty$, we obtain close to 2^m polynomials $F(z) \in \mathbb{U}_{n+m}$ that have $M(F)$ just about the same as $M(F_1)$. So we should expect M_n to vary smoothly with n. A modification of the argument that led to (4) can be used to show that one can also alter many coefficients of a given $F(z) \in \mathbb{U}_m$ without affecting $M(F)$ significantly, so that there will be many polynomials in $\mathbb{U}_n$ with $M(F)$ close to M_n.

One can obtain even stronger results by invoking the work of Spencer [34], who showed that there are exponentially many $F(z) \in \mathbb{U}_m$ with $M(F) < C$ for large constants C. This shows that in the construction above one can take $m = o(n)$, and not just $m = o(n/(\log n))$. Thus non-isolation of extremal polynomials is to be expected for high degrees. But the same argument also shows that sequences that achieve maximal merit factors cannot be isolated for large lengths. So why the difference in behavior for modest lengths? If we consider the effect that the change of a single coefficient can make for n on the order of 100, intuitively we might expect more isolation for extremal polynomials, and much more variation in M_n and M_n^* as n varies than is visible in Figures 1 and 2. Even the values of W_n and W_n^*, which show more variation, are surprisingly smooth.

Yet another puzzle is why M_n and M_n^* converge so much faster than W_n and W_n^*.

4 More general coefficients

Kahane showed that ultraflat polynomials do exist with $a_k \in \mathbf{C}, |a_k| = 1$. The computations of this paper strongly suggest such polynomials don't exist if we require $a_k = \pm 1$, but that there do exist constants $0 < \delta < C$ (even with $\delta = 0.5$ and $C = 1.5$) so that for all large n, there exist $F(z) \in \mathbb{U}_n$ with

$$\delta < |F(z)|/\sqrt{n+1} < C \tag{16}$$

for z on the unit circle. Beck [1] has shown, through a non-constructive argument, that there do exist polynomials satisfying (16) for some positive $\delta,\ C$ when the a_k are required to satisfy $a_k^{400} = 1$. (Higher orders of roots of unity lead to similar results.) So it is natural to conjecture that for each integer $r \ge 2$, if we require the a_k to be r-th roots of unity, the limits corresponding to M and m will exist, and will go to 1 as $r \to \infty$.

Some small scale computations for $r = 3, 4$ do support the conjecture about existence of the limits. They also show that for $r = 3$, it is harder to approach flatness than it is for the $r = 2$ (± 1) case, and that $r = 4$ does not produce polynomials much flatter than $r = 2$, at least for small degrees.

5 Polynomials that are never too small

GRS polynomials show that M_n is bounded. However, it is not known whether m_n is bounded away from zero, even for a sparse sequence of degrees n. The best known results come from a recursive construction of Carroll, Eustice, and Figiel [7]. If $F(z) \in \mathbb{U}_n$, and $m(F) \geq \alpha$, then

$$F(z^{n+1})F(z) \in \mathbb{U}_{(n+1)^2-1} \tag{17}$$

and for $|z| = 1$,

$$|F(z^{n+1})F(z)| \geq \alpha^2. \tag{18}$$

Repeating this construction, we obtain a sequence of polynomials $G(z)$ of degrees $r = (n+1)^k - 1$ with $m(G) \geq \alpha^k$, which gives

$$m_r \geq (r+1)^{-\beta}, \tag{19}$$

where

$$\beta = \frac{1}{2} - (\log \alpha)/(\log(n+1)). \tag{20}$$

The smallest value of β that has been found among all the polynomials examined so far comes from the Barker polynomial of degree 12, which has $m(F) = 0.8375,\ \alpha = 3.0196$ and gives $\beta = 0.069$. (This example was already featured in [7].) It is disappointing that even the skew-symmetric polynomials with $m(F) = m_n^*$ for $n = 100,\ 102$, and 104 do not provide a better bound. If the conjecture about the limit of m_n being about 0.64 is valid, and the limit is approached as smoothly as suggested by Fig. 1, it will require an example with the degree n on the order of 500 to improve on the Barker example of degree 12. This provides yet another demonstration of the uniqueness and nice behavior of Barker sequences.

Carroll, Eustice, and Figiel [7] have shown, using an interpolation procedure, that lower bounds similar to (19) hold for all large degrees r, not just for $r = 13^k - 1$.

6 Uniform distribution conjectures

B. Saffari and H. Montgomery developed conjectures about uniform distribution of GRS polynomials, cf. [25]. These have been proved recently, see [8,29], so we now know that as the degrees of GRS polynomials $F(z)$ grow, the values of $F(z)/\sqrt{n+1}$ as z runs over the unit circle approach the uniform distribution in the disk of radius $\sqrt{2}$.

For the polynomials $F(z)$ that are conjectured here to exist with $M(F) < 1.3$, say, the distribution of values cannot be uniform in this sense, as the L_2-norm of $F(z)/\sqrt{n+1}$ would be < 1. If we look at the distribution of values of the skew-symmetric polynomial of degree $n = 102$ that has the smallest maximal value, pictured in Fig. 4, we see there the expected concentration close to the unit circle.

If $F(z)/\sqrt{n+1}$ were to have its values approximately uniformly distributed in an annulus with radii $r < R$, the L_2-norm would be

$$(R^2 + r^2)/2$$

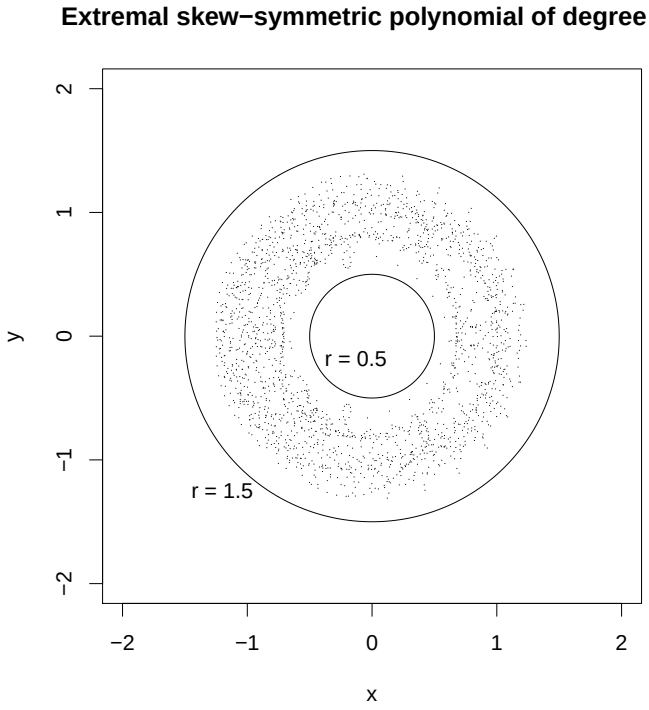

Fig. 5. Real and imaginary parts of the polynomial of degree 94 that achieves $W(F) = W_{94}$ at 2,000 points uniformly spread over the unit circle, scaled by $\sqrt{95}$, and circles of radii 0.5 and 1.5.

so for it to equal 1, we would need

$$r = \sqrt{2 - R^2}. \tag{21}$$

Fig. 5 shows the behavior on the unit circle of the skew-symmetric polynomial $F(z)$ of degree 94 that has $W(F) = 0.733...$ and thus fits in the smallest annulus of all skew-symmetric polynomials of degrees $72 \le n \le 104$. Whether that approximates a uniform distribution is difficult to say. This polynomial has $M(F) = 1.3162...$ and $m(F) = 0.5830...$, so does not fit the formula (21) too well, since substituting $R = 1.3162$ in that formula produces $r = 0.5173...$. Thus we do not have much evidence to suggest whether uniform distribution will prevail in the limit.

7 Algorithms

Computations were carried out with a simple program that examined all candidates (after taking advantage of the symmetries of (11)). If we write $F(z) = F_1(z) + F_2(z)$, where

$$F_1(z) = \sum_{k=0}^{15} a_k z^k,$$

say, then the values of $F_1(z)$ for all possible choices of $F_1(z)$ were precomputed at a small set of points on the upper half of the unit circle (typically 32 values). A candidate for $F_2(z)$ was evaluated at those points (with cosine evaluations replaced by table lookups, since only a small number of arguments were relevant), and choices of $F_1(z)$ that produced values of $F(z)$ that were either too small or too large were discarded. Thus the bulk of the computation consisted of adding values from two tables. Those few candidates that survived this simple winnowing process were then examined more carefully.

Considerably more efficient algorithms could be written, utilizing approaches similar to those in [5,26,27]. Typically, because of (4), a combination of particular $F_1(z)$ and $F_2(z)$ gives a large value at at least one of a small number of judiciously chosen points z with $|z| = 1$. In that case it is unnecessary to examine other combinations that differ from the given one in a small number of coefficients. A similar argument applies to small values.

Computations were carried out primarily on a variety of student lab machines, each of which typically had 4 cores in their Intel processors, which ran at about 3 GHz. Programs were run at the lowest possible priority, so as not to interfere with student work. The small memory requirements helped keep the programs' operation unobtrusive. Total run time was on the order of 30 years on a single core.

8 Completeness and correctness of results

The values of $m(F), M(F)$, and $W(F)$ for the polynomials in the tables are trustworthy. They were computed for the candidates identified by the main program with an inefficient but straightforward program. It used the trivial bounds on the first and second derivatives of $F(z)$ to find the extremal values.

What is not completely certain is whether all extremal polynomials were found. Typically around 100 cores were doing the searches, sending the promising candidates to a file over a local area network. This took several months in all, and there were some network hitches that triggered warnings that led to repeats of some computations. There is a chance that some network or storage system abnormalities may not have been detected, so that some good polynomials may have been missed. This probability is slight, though, since extremal polynomials are so rare.

9 Conclusions

The computations of this paper support the conjecture that ultraflat polynomials with ± 1 coefficients do not exist. However, it seems extremely likely that the Golay-Rudin-Shapiro polynomials are far from best possible in terms of never being large.

It is to be hoped that the extremal polynomials produced by this project will be helpful in finding some patterns that will lead to rigorous constructions.

The approach of the measures M_n, m_n, and W_n to their asymptotic values is surprisingly rapid. It was also unexpected that there would be as many polynomials close to the extremal ones.

Acknowledgments

Thanks are due to Enrico Bombieri, Charles Jackson, Stephan Mertens, Hugh Montgomery, and Michael Mossinghoff for their comments and helpful information.

The author acknowledges the Minnesota Supercomputing Institute (MSI) at the University of Minnesota for providing resources that contributed to the research results reported within this paper. The hospitality of the Institute for Mathematics and its Applications (IMA), also at the University of Minnesota, during part of the time this research was carried out, is also greatly appreciated.

References

1. J. Beck, "Flat polynomials on the unit circle—Note on a problem of Littlewood," *Bull. London Math. Soc.,* vol. 23, 1991, pp. 269–277.
2. E. Bombieri and J. Bourgain, "On Kahane's ultraflat polynomials," *J. European Math. Soc.,* vol. 11, 2009, pp. 627–703.
3. P. Borwein, *Computational Excursions in Analysis and Number Theory,* Springer, 2002.
4. P. Borwein and M. Mossinghoff, "Barker sequences and flat polynomials," pp. 71–88 in *Number Theory and Polynomials,* London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, 2008. Available at ⟨http://academics.davidson.edu/math/mossinghoff/BarkerSeqsFlatPolys_BorMoss.pdf⟩.
5. B. Bošković, F. Brglez, J. Brest, "Low-autocorrelation binary sequences: On improved merit factors and runtime predictions to achieve them," *Applied Soft Computing,* vol. 56, July 2017, pp. 262–285.
6. J. Brillhart and P. Morton, "A case study in mathematical research: The Golay-Rudin-Shapiro sequence," *Am. Math. Monthly,* vol. 103, Dec. 1996, pp. 854–869.
7. F. W. Carroll, D. Eustice, and T. Figiel, "The minimum modulus of polynomials with coefficients of modulus one," *J. London Math. Soc.,* ser. 2, vol. 16, 1977, pp. 76–82.
8. S. B. Ekhad and D. Zeilberger, "Integrals involving Rudin-Shapiro polynomials and a sketch of a proof of Saffari's conjecture," 2016 preprint, available at ⟨https://arxiv.org/abs/1605.06679⟩.
9. E. H. el Abdalaoui, "On the Erdős flat polynomials problem, Chowla conjecture and Riemann Hypothesis," preprint, version 2, 11 January 2017, available at ⟨https://arxiv.org/abs/1609.03435⟩.
10. T. Erdélyi, "On the flatness of conjugate reciprocal unimodular polynomials," *J. Math. Anal. Appl.,* vol. 432, no. 2, 2015, pp. 699–714.
11. P. Erdős, "Some unsolved problems," *Michigan Math. J.*, vol. 4, 1957, pp. 291–300.
12. P. Fan and M. Darnell, *Sequence Design for Communications Applications,* Research Studies Press, 1996.
13. A. Gersho, B. Gopinath, and A. Odlyzko, "Coefficient inaccuracy in transversal filtering," *Bell System Tech. J.,* vol. 58, 1979, pp. 2301–2316.
14. M. J. E. Golay, "Static multislit spectrometry and its application to the panoramic display of infrared spectra," *J. Optical Society of America,* vol. 41, 1951, pp. 468–472.

15. M. J. E. Golay, "The merit factor of long low autocorrelation binary sequences," *IEEE Trans. Information Theory,* vol. IT-28, no. 3, 1982, pp. 543–549.
16. S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar,* Cambridge Univ. Press, 2005.
17. G. Halasz, "On a result of Salem and Zygmund concerning random polynomials," *Studia Scient. Math. Hungar.,* vol. 8, 1973, pp. 369–377.
18. J. Jedwab, D. J. Katz, and K.-W. Schmidt, "Advances in the merit factor problem for binary sequences," *J. Combinatorial Theory, Series A,* vol. 120, 2013, pp. 882–906.
19. J.-P. Kahane, "Sur les polynômes à coefficients unimodulaires," *Bull. London Math. Soc.,* vol. 12, 1980, pp. 321–342.
20. T. W. Körner, "On a polynomial of Byrnes," *Bull. London Math. Soc.,* vol. 12, 1980, pp. 219–224.
21. K. H. Leung and B. Schmidt, "The anti-field-descent method," *J. Combinatorial Theory, Series A,* vol. 139, April 2016, pp. 87–131.
22. J. E. Littlewood, "On polynomials $\sum \pm z^m, \sum e^{\alpha m i}, z = e^{\theta i}$," *J. London Math. Soc.,* vol. 41, 1966, pp. 367–376.
23. J. E. Littlewood, *Some Problems in Real and Complex Analysis,* Heath, 1968.
24. I. D. Mercer, *Autocorrelation and Flatness of Height One Polynomials,* Ph.D. thesis, Simon Fraser University, 2005. Available at ⟨http://people.math.sfu.ca/∼idmercer/thesis.pdf⟩.
25. H. L. Montgomery, "Littlewood polynomials," in *Number Theory: In Honor of Krishna Alladi's 60-th Birthday,* G. Andrews and F. Gravan, eds., Springer, to appear.
26. T. Packebusch and S. Mertens, "Low autocorrelation binary sequences," *J. Physics A: Mathematical and Theoretical,* vol. 49, 2016, 165001.
27. S. D. Prestwich, "Improved branch-and-bound for low autocorrelation binary sequences," available at ⟨http://arxiv.org/abs/1305.6187⟩.
28. L. Robinson, *Polynomials with Plus or Minus One Coefficients: Growth Properties on the Unit Circle,* M.S. thesis, Simon Fraser University, 1997. Available at ⟨http://summit.sfu.ca/system/files/iritems1/7393/b18765270.pdf⟩.
29. B. Rodgers, "On the distribution of Rudin-Shapiro polynomials," 2016 preprint, available at ⟨http://arxiv.org/abs/1606.01637⟩.
30. W. Rudin, "Some theorems on Fourier coefficients," *Proc. Amer. Math. Soc.*, vol. 10, 1959, pp. 855–859.
31. B. Saffari, "Some polynomial extremal problems which emerged in the twentieth century," pp. 201–233 in J. S. Byrnes, ed., *Twentieth Century Harmonic Analysis – A Celebration,* Kluwer, 2001.
32. M. R. Schroeder, *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Biology, Digital Information, and Computing,* Springer, 1984.
33. H. S. Shapiro, *Extremal Problems for Polynomials and Power Series,* M.S. thesis, MIT, 1951.
34. J. Spencer, "Six standard deviations suffice," *Trans. Amer. Math. Soc.*, vol. 289, no. 2, June 1985, pp. 679–706.
35. N. Xiang and G. M. Sessler, eds., *Acoustics, Information, and Communication: Memorial Volume in Honor of Manfred R. Schroeder,* Springer, 2014.