Autocorrelation and Flatness of Height One Polynomials

Idris David Mercer

PhD Thesis Defence
April 25, 2005
HEIGHT ONE POLYNOMIAL:

Any polynomial of the form

\[ \alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \]

where \(|a_j| \leq 1\) for each \(j\).

Examples:

\[ \beta(z) = +1 + z + z^2 + z^3 + z^4 - z^5 - z^6 \]
\[ + z^7 + z^8 - z^9 + z^{10} - z^{11} + z^{12}, \]

\[ \sigma(z) = +1 + z + z^3 + z^7 + z^{12}, \]

\[ \lambda(z) = +1 + z - z^3 - z^4 - z^5 \]
\[ - z^6 - z^7 + z^9 + z^{10}. \]
Two important special cases:

**LITTLEWOOD POLYNOMIAL:**

\[ a_j \in \{-1, +1\} \text{ for each } j. \]

**ZERO-ONE POLYNOMIAL:**

\[ a_j \in \{0, 1\} \text{ for each } j. \]

From the previous slide:

\[ \beta(z) \] is a Littlewood polynomial,

\[ \sigma(z) \] is a zero-one polynomial,

\[ \lambda(z) \] is neither.
We define

$$\mathbb{S} := \{z \in \mathbb{C} : |z| = 1\},$$

the unit circle in the complex plane.

**UNDERLYING THEME**

(vague form)

Which Littlewood polynomials (or zero-one polynomials) are ‘flattest’ on $\mathbb{S}$?

If our domain of interest is $\mathbb{S}$, we’re actually considering functions of a **real** variable. If we let $t \in \mathbb{R}$ increase from 0 to $2\pi$, then $z := e^{it}$ goes ‘once around’ the unit circle.
EXAMPLE 1

The zero-one polynomial

\[ \sigma(z) = +1 + z + z^3 + z^7 + z^{12} \]

is a ‘flatter’ function on $S$ than

\[ \tau(z) = +1 + z^3 + z^6 + z^9 + z^{12}. \]
EXAMPLE 2

The Littlewood polynomial $\beta(z)$ defined on the first slide, with coefficient sequence

$$++ + + - - + + - + - + ,$$

is ‘flatter’ on $S$ than the polynomial given by

$$++ - + + - + + - + + - + .$$

(Notice that $\sigma(z)$ and $\tau(z)$ from Example 1 could also be written as

$$1101000100001$$

and

$$1001001001001$$

respectively.)
Some notation

We define

\[ L_n := \{a_0 + \cdots + a_{n-1}z^{n-1} : a_j \in \{\pm 1\} \ \forall j\} \]
\[ A_n := \{a_0 + \cdots + a_{n-1}z^{n-1} : a_j \in \{0, 1\} \ \forall j\} \]

so \(|L_n| = |A_n| = 2^n\). We also define

\[ A_{n,m} := \{\alpha(z) \in A_n : \alpha(1) = m\} \]

which is the set of polynomials in \(A_n\) such that precisely \(m\) of the coefficients are 1.
Among the $2^n$ polynomials in $\mathcal{L}_n$, or the $\binom{n}{m}$ polynomials in $\mathcal{A}_{n,m}$, which is ‘flattest’ on $\mathbb{S}$?

‘Flattest’ could mean w.r.t. one of the usual $L_p$ norms,

$$
\|\alpha\|_p := \left(\frac{1}{2\pi} \int_0^{2\pi} |\alpha(e^{it})|^p \, dt \right)^{1/p}.
$$

(Intuitively, $\|\alpha\|_p$ is the $p$th root of the average over $\mathbb{S}$ of the $p$th power of the modulus of $\alpha$.)
There turns out to be a relationship between the ‘flatness’ of a polynomial in $\mathcal{L}_n$ or $\mathcal{A}_n$ and certain combinatorial features of its coefficient sequence.

Loosely speaking, the ‘flat’ polynomials come from coefficient sequences that are not very ‘periodic’.

To describe this in more detail, we introduce the concept of \textit{autocorrelation}.
Given $n \in \mathbb{Z}^+$ and $A := (a_0, \ldots, a_{n-1}) \in \mathbb{R}^n$, we define the autocorrelations of $A$, for $0 \leq k \leq n - 1$, by

$$c_k := \sum_{j=0}^{n-k-1} a_j a_{j+k}.$$ 

For example, if $n = 8$ and $k = 3$, we have

$$c_3 = a_0a_3 + a_1a_4 + a_2a_5 + a_3a_6 + a_4a_7.$$
Example:

Autocorrelations of $+++\ -\ +$

<table>
<thead>
<tr>
<th>$+$</th>
<th>$+$</th>
<th>$+$</th>
<th>$-$</th>
<th>$+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$+$</td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
<td>$+$</td>
</tr>
</tbody>
</table>

$c_1 = +1 + 1 - 1 - 1 = 0$

<table>
<thead>
<tr>
<th>$+$</th>
<th>$+$</th>
<th>$+$</th>
<th>$-$</th>
<th>$+$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$+$</td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
</tr>
</tbody>
</table>

$c_2 = +1 - 1 + 1 = 1$

<table>
<thead>
<tr>
<th>$+$</th>
<th>$+$</th>
<th>$+$</th>
<th>$-$</th>
<th>$+$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$+$</td>
<td>$+$</td>
<td>$-$</td>
</tr>
</tbody>
</table>

$c_3 = -1 + 1 = 0$

<table>
<thead>
<tr>
<th>$+$</th>
<th>$+$</th>
<th>$+$</th>
<th>$-$</th>
<th>$+$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>$+$</td>
<td>$+$</td>
</tr>
</tbody>
</table>

$c_4 = +1 = 1$
The autocorrelations arise naturally when we consider the $L_p$ norms of $\alpha$ on $S$. This is true because for $z \in S$, we have

$$|\alpha(z)|^2 = \alpha(z)\overline{\alpha(z)}$$

$$= (a_0 + a_1z + \cdots + a_{n-1}z^{n-1})$$
$$\times (a_0 + a_1\frac{1}{z} + \cdots + a_{n-1}\frac{1}{z^{n-1}})$$

$$= c_{n-1}\frac{1}{z^{n-1}} + \cdots + c_1\frac{1}{z} + c_0 + c_1z + \cdots + c_{n-1}z^{n-1}.$$ 

Further straightforward computation reveals

$$\|\alpha\|_2^2 = a_0^2 + \cdots + a_{n-1}^2 = c_0,$$

$$\|\alpha\|_4^4 = c_0^2 + 2(c_1^2 + \cdots + c_{n-1}^2).$$
Probabilistic language

If $\Omega$ denotes one of the sets $L_n$, $A_n$, or $A_{n,m}$, then we can turn $\Omega$ into a probability space in the obvious way by giving each polynomial equal weight.

Then any function defined on $\Omega$ becomes a random variable, so it makes sense to ask about its expected value, variance, and so on.

Obvious examples of such random variables would include norms and autocorrelations.
Results in my thesis

Explicit formulae for average powers of norms and autocorrelations (Ch. 3 and 4)

Roots on $\mathbb{S}$ of Littlewood polynomials that have certain symmetries (Ch. 2)

Bounds on Turyn’s $b$ function, which measures ‘minimum maximum autocorrelation’ over all Littlewood polynomials of length $n$ (Ch. 3)

New proofs of old results: on cosine sums (Ch. 2) and Sidon sets (Ch. 4)
Explicit averages

If $\Omega$ is a set of polynomials, and $X$ is a function defined on $\Omega$, we write

$$E_\Omega(X) = \frac{1}{|\Omega|} \sum_{\alpha \in \Omega} X(\alpha),$$

or more briefly,

$$E(X) = \frac{1}{|\Omega|} \sum_{\alpha \in \Omega} X.$$

Some previous results:

$$E_{L_n}(\|\alpha\|_4^4) = 2n^2 - n,$$
$$E_{L_n}(\|\alpha\|_6^6) = 6n^3 - 9n^2 + 4n,$$
$$E_{L_n}(\|\alpha\|_8^8) = 24n^4 - 66n^3 + 58n^2 - 9n - 3 + 3(-1)^n.$$

The first is due to Newman & Byrnes and the next two are due to Borwein & Choi.
My explicit averages

For $k < n$, $\mathcal{E}_n(c_{n-k}^{2m})$ is a polynomial in $k$ of degree $m$. If we define

$$P_m(k) := \mathcal{E}_n(c_{n-k}^{2m}),$$

then we can generate the $P_m$ recursively via

$$P_{m+1}(k) = k^2P_m(k) - k(k - 1)P_m(k - 2).$$

For example, we have

$$P_1(k) = k,$$
$$P_2(k) = 3k^2 - 2k,$$
$$P_3(k) = 15k^3 - 30k^2 + 16k,$$
$$P_4(k) = 105k^4 - 420k^3 + 588k^2 - 272k.$$
Also, in a joint publication with Borwein & Choi, I show

\[ E_{A_n}(\|\alpha\|^4_4) = \frac{4n^3 + 42n^2 - 4n + 3 - 3(-1)^n}{96}, \]

\[ E_{A_{n,m}}(\|\alpha\|^4_4) = 2m^2 - m + \frac{2m[n^4]}{3(n-3)} + \frac{m[3](n-m)(2n^2 - 4n + 1 - (-1)^n)}{2n[n^4]}. \]

Here, \( x[k] \) is shorthand for \( x(x-1) \cdots (x-k+1) \).
Roots of special Littlewoods

Consider a Littlewood polynomial of odd length $2m + 1$,

$$\alpha(z) = a_0 + \cdots + a_m z^m + \cdots + a_{2m} z^{2m}.$$  

We call $\alpha$ **skewsymmetric** if we have

$$a_{m+j} = (-1)^j a_{m-j} \text{ for all } j \in \{1, \ldots, m\}.$$  

Exhaustive searches in Robinson’s thesis show that for all $n \in \{11, 13, \ldots, 25\}$, the polynomial in $\mathcal{L}_n$ with largest infimum on $S$ turns out to be skewsymmetric.

I used properties of Chebyshev polynomials to prove skewsymmetric Littlewood polynomials have no zeros on $S$. 

Bounds on Turyn’s \( b \) function

In 1968, Turyn defined

\[
    b(n) := \min_{\alpha \in \mathcal{L}_n} \max_{1 \leq k < n} |c_k|
\]

(so \( b(n) = 1 \) if and only if there is a Barker sequence of length \( n \)).

Engineers have performed exhaustive searches revealing that

\[
    b(n) \leq 2 \text{ for all } n \leq 21, \quad b(n) \leq 3 \text{ for all } n \leq 48, \quad b(n) \leq 4 \text{ for all } n \leq 69.
\]
The best previously known upper bound on $b(n)$ appears to be this 1968 result of Moon & Moser:

For all $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that

$$b(n) \leq (2 + \varepsilon)\sqrt{n \log n}$$

for all $n \geq N$.

I used refined Chernoff-type bounds for ‘tails’ of binomial distributions to improve this to

$$b(n) \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$
New proofs of known results

Any expression of the form
\[ \cos(n\theta) + a_{n-1} \cos((n-1)\theta) + \cdots + a_1 \cos(\theta), \]
where the \( a_j \) are real, must attain both of the values \(+1\) and \(−1\) as \( \theta \) ranges through \([0, \pi]\).

This has a short proof using complex analysis, but I found a proof without complex analysis that reproves results of Gilbert & Smyth on zero-mean cosine polynomials maintaining the same sign on ‘long’ intervals.
Ubiquity of Sidon sets

Suppose \( \{\beta_1, \ldots, \beta_m\} \subseteq [n] \), where \([n]\) is just shorthand for the set \(\{0, \ldots, n - 1\}\).

If the \(\binom{m}{2} \) positive differences \(\beta_i - \beta_j\) are all distinct, we call \(\{\beta_1, \ldots, \beta_m\}\) a **Sidon set**.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>3</th>
<th>7</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>6</td>
<td>4</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>-</td>
</tr>
</tbody>
</table>

\(\{0, 1, 3, 7, 12\}\) is a Sidon set.
The explicit formula for $E_{A_{n,m}}(\|\alpha\|_4^4)$ found in the joint paper with Borwein & Choi has a surprising consequence.

Using Markov’s inequality, we show that if $A$ is a randomly chosen $m$-subset of $[n]$, then

$$\Pr[A \text{ is Sidon}] > 1 - \frac{m^4}{3n}.$$  

Thus if $m = o(n^{1/4})$, the probability that $A$ is Sidon approaches 1 as $n$ approaches infinity.

This appears in papers by Godbole et al. and by Nathanson, but it is interesting that we get it for ‘free’ as a result of finding the ‘typical four-norm’ of a zero-one polynomial.
In closing,

‘Mr. Pibb is a replica of Dr. Pepper, but it’s a bullsh*t replica, ’cuz the dude didn’t even get his degree.’