Canad. Math. Bull. Vol. **51** (4), 2008 pp. 497–507

Expected Norms of Zero-One Polynomials

Peter Borwein, Kwok-Kwong Stephen Choi, and Idris Mercer

Abstract. Let $\mathcal{A}_n = \left\{ a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} : a_j \in \{0,1\} \right\}$, whose elements are called *zero-one polynomials* and correspond naturally to the 2^n subsets of $[n] := \{0, 1, \ldots, n-1\}$. We also let $\mathcal{A}_{n,m} = \{\alpha(z) \in \mathcal{A}_n : \alpha(1) = m\}$, whose elements correspond to the $\binom{n}{m}$ subsets of $[n]$ of size m, and let $\mathcal{B}_n = \mathcal{A}_{n+1} \setminus \mathcal{A}_n$, whose elements are the zero-one polynomials of degree exactly n.

Many researchers have studied norms of polynomials with restricted coefficients. Using $\|\alpha\|_p$ to denote the usual L_p norm of α on the unit circle, one easily sees that $\alpha(z) = a_0 + a_1 z + \cdots + a_N z^N \in \mathbb{R}[z]$ satisfies $\|\alpha\|_2^2 = c_0$ and $\|\alpha\|_4^4 = c_0^2 + 2(c_1^2 + \cdots + c_N^2)$, where $c_k := \sum_{j=0}^{N-k} a_j a_{j+k}$ for $0 \le k \le N$.

If $\alpha(z) \in \mathcal{A}_{n,m}$, say $\alpha(z) = z^{\beta_1} + \cdots + z^{\beta_m}$ where $\beta_1 < \cdots < \beta_m$, then c_k is the number of times k appears as a difference $\beta_i - \beta_j$. The condition that $\alpha \in \mathcal{A}_{n,m}$ satisfies $c_k \in \{0,1\}$ for $1 \le k \le n-1$ is thus equivalent to the condition that $\{\beta_1, \ldots, \beta_m\}$ is a *Sidon set* (meaning all differences of pairs of elements are distinct).

In this paper, we find the average of $\|\alpha\|_4^4$ over $\alpha \in \mathcal{A}_n$, $\alpha \in \mathcal{B}_n$, and $\alpha \in \mathcal{A}_{n,m}$. We further show that our expression for the average of $\|\alpha\|_4^4$ over $\mathcal{A}_{n,m}$ yields a new proof of the known result: if $m = o(n^{1/4})$ and $B(n,m)$ denotes the number of Sidon sets of size m in $[n]$, then almost all subsets of $[n]$ of size m are Sidon, in the sense that $\lim_{n\to\infty} B(n,m)/\binom{n}{m} = 1$.

1 Introduction and Statement of Main Result

We let $\mathcal{A}_n$ denote the set $\{a_0 + a_1 z + \cdots + a_{n-1}z^{n-1} : a_j \in \{0,1\} \text{ for all } j\}$, and we call the elements of $\mathcal{A}_n$ *zero-one polynomials*. There is a natural bijection between the 2^n polynomials in $\mathcal{A}_n$ and the 2^n subsets of $[n] := \{0, 1, \ldots, n-1\}$. Generally, if $\alpha(z) \in \mathcal{A}_n$, we define

$$m := \alpha(1) = \text{ the number of coefficients of } \alpha(z) \text{ that are 1},$$

and we write $\alpha(z) = z^{\beta_1} + z^{\beta_2} + \cdots + z^{\beta_m}$ where $\beta_1 < \beta_2 < \cdots < \beta_m$, so $\{\beta_1, \beta_1, \ldots, \beta_m\}$ is the subset of $[n]$ that corresponds to $\alpha(z)$. We let $\mathcal{A}_{n,m}$ denote the set $\{\alpha(z) \in \mathcal{A}_n : \alpha(1) = m\}$, so $|\mathcal{A}_{n,m}| = \binom{n}{m}$ and $\mathcal{A}_n = \mathcal{A}_{n,0} \cup \mathcal{A}_{n,1} \cup \cdots \cup \mathcal{A}_{n,n}$. We also define $\mathcal{B}_n := \mathcal{A}_{n+1} \setminus \mathcal{A}_n$, so $\mathcal{B}_n$ consists of the 2^n zero-one polynomials of degree exactly n.

A recurring theme in the literature is the problem of finding a polynomial with "small" norm subject to some restriction on its coefficients. (See [3, Problem 26], [5, Problem 19], or [1, Ch. 4, 15].) In general, for

$$\alpha(z) = a_0 + a_1 z + \cdots + a_N z^N \in \mathbb{R}[z], \tag{1.1}$$

Received by the editors May 29, 2006.
The research of Peter Borwein and Stephen Choi is supported by NSERC of Canada.
AMS subject classification: Primary: 11B83; secondary: 11C08, 30C10.

we define the usual L_p norms of $\alpha(z)$ on the unit circle:

$$\|\alpha\|_p := \Big(\frac{1}{2\pi}\int_0^{2\pi} \big|\alpha(e^{i\theta})\big|^p \, d\theta\Big)^{1/p},$$

where $p \geq 1$ is real. The main result of this paper, which appears as Theorem 4.1 in Section 4, is that if $n \geq 4$ and $m \leq n$, we have

$$\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \frac{4n^3 + 42n^2 - 4n + 3 - 3(-1)^n}{96},$$

$$\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(2n^2 - 4n + 1 - (-1)^n)}{2n^{[4]}},$$

$$\mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) = \frac{4n^3 + 66n^2 + 188n + 87 + 9(-1)^n}{96},$$

where $\mathbf{E}_\Omega(\|\alpha\|_4^4)$ denotes the average of $\|\alpha\|_4^4$ over the polynomials in Ω, and the notation $x^{[k]}$ is shorthand for $x(x-1)\cdots(x-k+1)$. This complements results of Newman and Byrnes [7], who found the average of $\|\alpha\|_4^4$ over the 2^n polynomials of the form

$$a_0 + a_1 z + \cdots + a_{n-1}z^{n-1}, \quad a_j \in \{+1, -1\} \text{ for all } j, \tag{1.2}$$

and Borwein and Choi [2], who found (among other things) the average of $\|\alpha\|_6^6$ and $\|\alpha\|_8^8$ over the 2^n polynomials of the form (1.2), and the average of $\|\alpha\|_2^2$, $\|\alpha\|_4^4$, and $\|\alpha\|_6^6$ over the 3^n polynomials of the form

$$a_0 + a_1 z + \cdots + a_{n-1}z^{n-1}, \quad a_j \in \{+1, 0, -1\} \text{ for all } j.$$

2 Autocorrelation

Notice that if α is of the form (1.1) and $|z| = 1$, we have

$$\begin{aligned}|\alpha(z)|^2 = \alpha(z)\overline{\alpha(z)} &= (a_0 + a_1 z + \cdots + a_N z^N)\Big(a_0 + a_1\frac{1}{z} + \cdots + a_N\frac{1}{z^N}\Big)\\ &= c_N\frac{1}{z^N} + \cdots + c_1\frac{1}{z} + c_0 + c_1 z + \cdots + c_N z^N,\end{aligned}$$

where the c_k are the so-called *(aperiodic) autocorrelations* of α, defined for $0 \leq k \leq N$ by $c_k := \sum_{j=0}^{N-k} a_j a_{j+k}$. Using the general fact that

$$\frac{1}{2\pi}\int_0^{2\pi}\Big(b_{-M}\frac{1}{z^M} + \cdots + b_{-1}\frac{1}{z} + b_0 + b_1 z + \cdots + b_M z^M\Big)\, d\theta = b_0, \quad (z = e^{i\theta}),$$

we see that for α of the form (1.1), we have

$$\|\alpha\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi}\Big(c_N\frac{1}{z^N} + \cdots + c_1\frac{1}{z} + c_0 + c_1 z + \cdots + c_N z^N\Big)\, d\theta = c_0, \quad (z = e^{i\theta}),$$

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

and

(2.1)
$$\|\alpha\|_4^4 = \frac{1}{2\pi}\int_0^{2\pi}\Big(c_N\frac{1}{z^N}+\cdots+c_1\frac{1}{z}+c_0+c_1z+\cdots+c_Nz^N\Big)^2 d\theta$$
$$= c_N^2+\cdots+c_1^2+c_0^2+c_1^2+\cdots+c_N^2 = c_0^2+2(c_1^2+\cdots+c_N^2), \quad (z=e^{i\theta}).$$

We further observe that

$$c_k^2 = \Big(\sum_{j=0}^{N-k} a_ja_{j+k}\Big)^2 = \sum_{i=0}^{N-k} a_ia_{i+k}\cdot\sum_{j=0}^{N-k} a_ja_{j+k} = \sum_{i=0}^{N-k}\sum_{j=0}^{N-k} a_ia_ja_{i+k}a_{j+k}$$
$$= \sum_{i=0}^{N-k}\sum_{j=0}^{N-k} f(i,j).$$

Noting that $f(i,j) := a_ia_ja_{i+k}a_{j+k}$ satisfies $f(i,j)=f(j,i)$, we have

$$(2.2)\qquad c_k^2 = \sum_{i=0}^{N-k}\sum_{j=0}^{N-k} f(i,j) = \sum_{i=0}^{N-k} f(i,i) + 2\sum_{0\le i<j\le N-k} f(i,j)$$
$$= \sum_{i=0}^{N-k} a_i^2a_{i+k}^2 + 2\sum_{0\le i<j\le N-k} a_ia_ja_{i+k}a_{j+k}.$$

If $\alpha(z) = a_0+\cdots+a_{n-1}z^{n-1} = z^{\beta_1}+\cdots+z^{\beta_m}\in\mathcal{A}_{n,m}$, then we have $c_0=m$ and c_k is the number of j such that a_j and a_{j+k} are both 1 and is equal to the number of times k appears as a difference $\beta_i-\beta_j$. Thus $c_1+\cdots+c_{n-1}=m(m-1)/2$, and since the c_k are nonnegative integers, we have

$$(2.3)\qquad c_1^2+\cdots+c_{n-1}^2 \ge c_1+\cdots+c_{n-1} = m(m-1)/2$$

with equality if and only if $c_k\in\{0,1\}$ for $1\le k\le n-1$, or in other words, if and only if all differences of pairs of elements of $\{\beta_1,\dots,\beta_m\}$ are distinct. If all differences of pairs of elements of $\{\beta_1,\dots,\beta_m\}$ are distinct, we call $\{\beta_1,\dots,\beta_m\}$ a *Sidon set*.

Using (2.1), we see that (2.3) and $c_0=m$ prove the following.

Proposition 2.1 *For any $\alpha(z)=z^{\beta_1}+\cdots+z^{\beta_m}\in\mathcal{A}_{n,m}$, we have $\|\alpha\|_4^4\ge 2m^2-m$, with equality if and only if $\{\beta_1,\dots,\beta_m\}$ is a Sidon set.*

We observe also that (2.3) implies that $c_1^2+\cdots+c_{n-1}^2-m(m-1)/2$ is a nonnegative integer, and is zero if and only if $\{\beta_1,\dots,\beta_m\}$ is Sidon.

3 Some Facts and Notation

If Ω denotes $\mathcal{A}_n$, $\mathcal{B}_n$, or $\mathcal{A}_{n,m}$, then we turn Ω into a probability space by giving each polynomial $\alpha\in\Omega$ equal weight $p(\alpha)$.

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

Generally, we will denote a typical element of $\mathcal{A}_n$ or $\mathcal{A}_{n,m}$ by

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

and denote a typical element of $\mathcal{B}_n$ by $\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} + z^n$. As in Section 1, if $\alpha \in \mathcal{A}_{n,m}$, we also write

$$\alpha(z) = z^{\beta_1} + z^{\beta_2} + \cdots + z^{\beta_m}$$

where $\beta_1 < \beta_2 < \cdots < \beta_m$.

If Ω is one of the three spaces $\mathcal{A}_n$, $\mathcal{B}_n$, or $\mathcal{A}_{n,m}$ and X is a random variable on Ω, we of course have $\mathbf{E}_\Omega(X) = \sum_{\alpha \in \Omega} X(\alpha) p(\alpha)$, and we will sometimes omit the subscript Ω if it is clear from the context what probability space we are considering.

Two facts we will use that are each immediate from first principles are *Markov's inequality*, $\mathbf{Pr}[X \geq a] \leq \mathbf{E}(X)/a$, where X is a nonnegative real random variable, and *linearity of expectation*, $\mathbf{E}(X_1 + \cdots + X_k) = \mathbf{E}(X_1) + \cdots + \mathbf{E}(X_k)$, which holds regardless of dependence or independence of the X_i.

4 Calculation of $\mathbf{E}(\|\alpha\|_4^4)$

Let j_1, j_2, j_3, j_4 denote distinct integers. We begin this section by finding some averages of products of a_{j_i} that we will need later. First, suppose our probability space Ω is $\mathcal{A}_n$. We then have

$$\mathbf{E}(a_{j_1} a_{j_2}) = \frac{1}{2^n}(\text{number of } \alpha \in \mathcal{A}_n \text{ such that } a_{j_1} = a_{j_2} = 1) = \frac{2^{n-2}}{2^n} = \frac{1}{4}, \tag{4.1}$$

and by similar reasoning, we have

$$\mathbf{E}(a_{j_1} a_{j_2} a_{j_3}) = 1/8, \quad \mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4}) = 1/16. \tag{4.2}$$

Now suppose our probability space Ω is $\mathcal{A}_{n,m}$. We then have

$$\begin{aligned} \mathbf{E}(a_{j_1} a_{j_2}) &= \frac{1}{\binom{n}{m}}(\text{number of } \alpha \in \mathcal{A}_{n,m} \text{ such that } a_{j_1} = a_{j_2} = 1) \\ &= \frac{\binom{n-2}{m-2}}{\binom{n}{m}} = \frac{m(m-1)}{n(n-1)} = \frac{m^{[2]}}{n^{[2]}}, \end{aligned} \tag{4.3}$$

and by similar reasoning, we have

$$\mathbf{E}(a_{j_1} a_{j_2} a_{j_3}) = m^{[3]}/n^{[3]}, \quad \mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4}) = m^{[4]}/n^{[4]}. \tag{4.4}$$

We note that we need $n \geq 4$ in order for all expressions in (4.3) and (4.4) to be defined. For $\Omega = \mathcal{A}_{n,m}$, the case $n \leq 3$ will be treated separately.

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

Now if Ω is either of the probability spaces $\mathcal{A}_n$ or $\mathcal{A}_{n,m}$, then equation (2.2) gives

$$c_k^2 = \sum_{i=0}^{n-k-1} a_i a_{i+k} + 2 \sum_{0 \le i < j \le n-k-1} a_i a_{i+k} a_j a_{j+k}. \tag{4.5}$$

We define $\lambda := n - k$ and also define

$$S := \sum_{i=0}^{\lambda-1} a_i a_{i+k}, \tag{4.6}$$

$$T := \sum_{0 \le i < j \le \lambda-1} a_i a_j a_{i+k} a_{j+k}, \tag{4.7}$$

which of course implies $c_k^2 = S + 2T$. If $k = 0$, then $c_k^2 = m^2$. So if $\Omega = \mathcal{A}_{n,m}$, we have simply $\mathbf{E}(c_0^2) = m^2$, whereas if $\Omega = \mathcal{A}_n$, we have

$$\mathbf{E}(c_0^2) = \sum_{m=0}^{n} \frac{\binom{n}{m}}{2^n} m^2. \tag{4.8}$$

It is an exercise to see that the right side of (4.8) evaluates to $(n^2 + n)/4$. Alternatively, we may observe that c_0 has a binomial distribution with parameters n and $1/2$, which implies

$$\mathbf{E}(c_0^2) = \mathbf{Var}(c_0) + \mathbf{E}(c_0)^2 = n \cdot \frac{1}{2} \cdot \frac{1}{2} + \left(n \cdot \frac{1}{2}\right)^2 = \frac{n^2 + n}{4}. \tag{4.9}$$

Having found $\mathbf{E}(c_0^2)$ for $\Omega = \mathcal{A}_{n,m}$ and for $\Omega = \mathcal{A}_n$, we now shift our attention to $\mathbf{E}(c_k^2)$ for $k \ne 0$.

Assume $k \ne 0$, and observe that (4.5), (4.6), and (4.7) (and linearity of expectation) give us

$$\mathbf{E}(c_k^2) = \mathbf{E}(S) + 2\mathbf{E}(T) = \sum_{i=0}^{\lambda-1} \mathbf{E}(a_i a_{i+k}) + 2 \sum_{0 \le i < j \le \lambda-1} \mathbf{E}(a_i a_j a_{i+k} a_{j+k}). \tag{4.10}$$

Since $k \ne 0$, each of the λ terms in the sum $\mathbf{E}(S)$ is of the form $\mathbf{E}(a_{j_1} a_{j_2})$ where $j_1 \ne j_2$. We thus have

$$\mathbf{E}(S) = \begin{cases} \lambda/4 & \text{if } \Omega = \mathcal{A}_n, \\ \lambda m^{[2]}/n^{[2]} & \text{if } \Omega = \mathcal{A}_{n,m}, \end{cases} \tag{4.11}$$

by (4.1) and (4.2). As for the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$, each term is of the form $\mathbf{E}(a_i a_j a_{i+k} a_{j+k})$. Since $k \ne 0$ and $i < j$, the four subscripts $i, j, i+k, j+k$ constitute either three distinct integers (if $j = i + k$) or four distinct integers (if $j \ne i + k$). If $\{i, j, i+k, j+k\}$ consists of three distinct integers j_1, j_2, j_3 where j_3 is the one that is

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

"repeated", then, since $a_j \in \{0,1\}$ for all j, we have $\mathbf{E}(a_i a_j a_{i+k} a_{j+k}) = \mathbf{E}(a_{j_1} a_{j_2} a_{j_3}^2) = \mathbf{E}(a_{j_1} a_{j_2} a_{j_3})$, whereas, of course, if $\{i, j, i+k, j+k\}$ consists of four distinct integers, then $\mathbf{E}(a_i a_j a_{i+k} a_{j+k})$ is of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$. Therefore, we now ask the question: For which of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ does the set $\{i, j, i+k, j+k\}$ consist of only three distinct integers?

For some $i \in \{0, 1, \ldots, \lambda-1\}$, there is exactly one j satisfying both $i < j \leq \lambda - 1$ and $j = i + k$, and for other values of i, there is no such j. We will say that i is of "type I" if the former criterion holds, and is of "type II" if the latter criterion holds. An integer i is of type I if and only if $i + k < \lambda$, or equivalently, $i < \lambda - k = n - 2k$. If $n - 2k \leq 0$ (*i.e.*, if $k \geq \lceil n/2 \rceil$), then $i < n - 2k$ never happens, *i.e.*, no i is of type I and so all of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$. On the other hand, if $n - 2k > 0$ (*i.e.*, if $k < \lceil n/2 \rceil$), then $i < n - 2k = \lambda - k$ sometimes happens; namely, it happens if and only if i is one of the $\lambda - k$ integers $0, 1, \ldots, \lambda - k - 1$. In that case, each of those $\lambda - k$ values of i is of type I, which implies that precisely $\lambda - k$ of the $\binom{\lambda}{2}$ terms in the sum $\mathbf{E}(T)$ are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3})$ and the remaining terms are of the form $\mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})$.

This implies that we have

$$\mathbf{E}(T) = \begin{cases} \binom{\lambda}{2} \mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4}) & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2} \mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4}) & \\ \qquad + (\lambda - k)\big[\mathbf{E}(a_{j_1} a_{j_2} a_{j_3}) - \mathbf{E}(a_{j_1} a_{j_2} a_{j_3} a_{j_4})\big] & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

Thus, if $\Omega = \mathcal{A}_n$, then

$$\mathbf{E}(T) = \begin{cases} \binom{\lambda}{2}/16 & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2}/16 + (\lambda - k)/16 & \text{if } k < \lceil n/2 \rceil, \end{cases}$$

and hence by (4.10) and (4.11),

$$\mathbf{E}(c_k^2) = \begin{cases} \lambda/4 + \lambda(\lambda - 1)/16 & \text{if } k \geq \lceil n/2 \rceil, \\ \lambda/4 + \lambda(\lambda - 1)/16 + 2(\lambda - k)/16 & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

On the other hand, if $\Omega = \mathcal{A}_{n,m}$, then

$$\mathbf{E}(T) = \begin{cases} \binom{\lambda}{2} m^{[4]}/n^{[4]} & \text{if } k \geq \lceil n/2 \rceil, \\ \binom{\lambda}{2} m^{[4]}/n^{[4]} + (\lambda - k)[m^{[3]}/n^{[3]} - m^{[4]}/n^{[4]}] & \text{if } k < \lceil n/2 \rceil, \end{cases}$$

and hence

$$\mathbf{E}(c_k^2) = \begin{cases} \lambda \frac{m^{[2]}}{n^{[2]}} + \lambda(\lambda - 1) \frac{m^{[4]}}{n^{[4]}} & \text{if } k \geq \lceil n/2 \rceil, \\ \lambda \frac{m^{[2]}}{n^{[2]}} + \lambda(\lambda - 1) \frac{m^{[4]}}{n^{[4]}} + 2(\lambda - k)\big[\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\big] & \text{if } k < \lceil n/2 \rceil. \end{cases}$$

It then follows that if $\Omega = \mathcal{A}_n$, we have

$$\text{(4.12)} \quad \mathbf{E}(c_1^2 + \cdots + c_{n-1}^2) = \sum_{k=1}^{n-1} \Big(\frac{\lambda}{4}\Big) + \sum_{k=1}^{n-1} \Big(\frac{\lambda(\lambda - 1)}{16}\Big) + \sum_{k=1}^{\lceil n/2 \rceil - 1} \Big(\frac{2(\lambda - k)}{16}\Big),$$

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

whereas if $\Omega = \mathcal{A}_{n,m}$, we have

$$\text{(4.13)}\quad \mathbf{E}(c_1^2 + \cdots + c_{n-1}^2) = \sum_{k=1}^{n-1}\Big(\lambda \frac{m^{[2]}}{n^{[2]}}\Big) + \sum_{k=1}^{n-1}\Big(\lambda(\lambda-1)\frac{m^{[4]}}{n^{[4]}}\Big) + \sum_{k=1}^{\lceil n/2\rceil -1}\Big(2(\lambda-k)\Big[\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\Big]\Big).$$

Recalling that λ is simply shorthand for $n-k$, it is straightforward to verify that

$$\sum_{k=1}^{n-1}\lambda = \frac{n(n-1)}{2}, \quad \sum_{k=1}^{n-1}(\lambda^2-\lambda) = \frac{n(n-1)(n-2)}{3},$$

and that

$$\sum_{k=1}^{\lceil n/2\rceil -1} 2(\lambda-k) = \begin{cases} n(n-2)/2 & \text{if } n \text{ is even,}\\ (n-1)^2/2 & \text{if } n \text{ is odd.}\end{cases}$$

So, if $\Omega = \mathcal{A}_n$, then from (4.12) we get

$$\mathbf{E}(c_1^2 + \cdots + c_{n-1}^2) = \begin{cases} \frac{1}{4}\cdot\frac{n(n-1)}{2} + \frac{1}{16}\cdot\frac{n(n-1)(n-2)}{3} + \frac{1}{16}\cdot\frac{n(n-2)}{2} & \text{if } n \text{ is even,}\\ \frac{1}{4}\cdot\frac{n(n-1)}{2} + \frac{1}{16}\cdot\frac{n(n-1)(n-2)}{3} + \frac{1}{16}\cdot\frac{(n-1)^2}{2} & \text{if } n \text{ is odd,}\end{cases}$$
$$= \begin{cases} (2n^3+9n^2-14n)/96 & \text{if } n \text{ is even,}\\ (2n^3+9n^2-14n+3)/96 & \text{if } n \text{ is odd,}\end{cases}$$

which, using (2.1) and (4.9), implies

$$\mathbf{E}(\|\alpha\|_4^4) = \begin{cases} \frac{n^2+n}{4} + \frac{2n^3+9n^2-14n}{48} = \frac{2n^3+21n^2-2n}{48} & \text{if } n \text{ is even,}\\ \frac{n^2+n}{4} + \frac{2n^3+9n^2-14n+3}{48} = \frac{2n^3+21n^2-2n+3}{48} & \text{if } n \text{ is odd,}\end{cases}$$

or equivalently

$$\text{(4.14)}\quad \mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \frac{4n^3+42n^2-4n+3-3(-1)^n}{96}.$$

On the other hand, if $\Omega = \mathcal{A}_{n,m}$, then from (4.13) we get

$$\mathbf{E}(c_1^2 + \cdots + c_{n-1}^2)$$
$$= \begin{cases} \frac{m^{[2]}}{n^{[2]}}\cdot\frac{n(n-1)}{2} + \frac{m^{[4]}}{n^{[4]}}\cdot\frac{n(n-1)(n-2)}{3} + \Big(\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\Big)\cdot\frac{n(n-2)}{2} & \text{if } n \text{ is even,}\\ \frac{m^{[2]}}{n^{[2]}}\cdot\frac{n(n-1)}{2} + \frac{m^{[4]}}{n^{[4]}}\cdot\frac{n(n-1)(n-2)}{3} + \Big(\frac{m^{[3]}}{n^{[3]}} - \frac{m^{[4]}}{n^{[4]}}\Big)\cdot\frac{(n-1)^2}{2} & \text{if } n \text{ is odd,}\end{cases}$$
$$= \begin{cases} \binom{m}{2} + m^{[4]}/(3(n-3)) + m^{[3]}(n-m)(n^2-2n)/(2n^{[4]}) & \text{if } n \text{ is even,}\\ \binom{m}{2} + m^{[4]}/(3(n-3)) + m^{[3]}(n-m)(n^2-2n+1)/(2n^{[4]}) & \text{if } n \text{ is odd,}\end{cases}$$

which, using (2.1), implies

$$\mathbf{E}(\|\alpha\|_4^4) = \begin{cases} 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n)}{n^{[4]}} & \text{if } n \text{ is even,} \\ 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n+1)}{n^{[4]}} & \text{if } n \text{ is odd,} \end{cases}$$

or equivalently

$$(4.15)\quad \mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(2n^2-4n+1-(-1)^n)}{2n^{[4]}}.$$

Notice that if m is fixed and n approaches infinity, then $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$ approaches $2m^2 - m$, *i.e.*, for fixed m and large n, we expect a random $\alpha \in \mathcal{A}_{n,m}$ to correspond to a Sidon set, as is consistent with intuition.

If $\Omega = \mathcal{B}_n$, since $\mathcal{B}_n := \mathcal{A}_{n+1} \setminus \mathcal{A}_n$, we get

$$\begin{aligned} \mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) &= \frac{1}{2^n} \sum_{\alpha \in \mathcal{B}_n} \|\alpha\|_4^4 = 2\mathbf{E}_{\mathcal{A}_{n+1}}(\|\alpha\|_4^4) - \mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) \\ &= \frac{4n^3 + 66n^2 + 188n + 87 + 9(-1)^n}{96} \end{aligned}$$

by (4.14). Therefore we have proved

Theorem 4.1 *If $m \le n$, we have*

$$\mathbf{E}_{\mathcal{A}_n}(\|\alpha\|_4^4) = \frac{4n^3 + 42n^2 - 4n + 3 - 3(-1)^n}{96},$$

$$\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) = 2m^2 - m + \frac{2m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(2n^2-4n+1-(-1)^n)}{2n^{[4]}} \quad (\text{if } n \ge 4),$$

$$\mathbf{E}_{\mathcal{B}_n}(\|\alpha\|_4^4) = \frac{4n^3 + 66n^2 + 188n + 87 + 9(-1)^n}{96}.$$

For completeness, we also determine $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$ when $n \le 3$. If $n \le 3$, we have $\alpha(z) = a_0 + a_1 z + a_2 z^2$ and then

$$\begin{aligned} \|\alpha\|_4^4 &= c_0^2 + 2c_1^2 + 2c_2^2 \\ &= (a_0^2 + a_1^2 + a_2^2)^2 + 2(a_0a_1 + a_1a_2)^2 + 2(a_0a_2)^2 \\ &= a_0^4 + a_1^4 + a_2^4 + 4(a_0^2a_1^2 + a_0^2a_2^2 + a_1^2a_2^2) + 4a_0a_1^2a_2 \\ &= a_0 + a_1 + a_2 + 4(a_0a_1 + a_0a_2 + a_1a_2) + 4a_0a_1a_2, \end{aligned}$$

since $a_j \in \{0, 1\}$ from which it readily follows that

$$\begin{aligned} \mathbf{E}_{\mathcal{A}_{2,0}}(\|\alpha\|_4^4) &= \mathbf{E}_{\mathcal{A}_{3,0}}(\|\alpha\|_4^4) = 0, \\ \mathbf{E}_{\mathcal{A}_{2,1}}(\|\alpha\|_4^4) &= \mathbf{E}_{\mathcal{A}_{3,1}}(\|\alpha\|_4^4) = 1, \\ \mathbf{E}_{\mathcal{A}_{2,2}}(\|\alpha\|_4^4) &= \mathbf{E}_{\mathcal{A}_{3,2}}(\|\alpha\|_4^4) = 6, \\ \mathbf{E}_{\mathcal{A}_{3,3}}(\|\alpha\|_4^4) &= 19. \end{aligned}$$

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

We remark that substituting $m \in \{0, 1, 2, 3\}$ into the second equation in Theorem 4.1 and then formally cancelling common factors as appropriate, we get

$$\mathbf{E}_{\mathcal{A}_{n,3}}(\|\alpha\|_4^4) = 15 + \frac{3(2n^2 - 4n + 1 - (-1)^n)}{n(n-1)(n-2)},$$
$$\mathbf{E}_{\mathcal{A}_{n,2}}(\|\alpha\|_4^4) = 6,$$
$$\mathbf{E}_{\mathcal{A}_{n,1}}(\|\alpha\|_4^4) = 1,$$
$$\mathbf{E}_{\mathcal{A}_{n,0}}(\|\alpha\|_4^4) = 0,$$

yielding results consistent with the explicit averages just obtained for $n \leq 3$.

5 Ubiquity of Sidon Sets

We show that our expression for $\mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4)$ yields a new proof of a result that appears in articles by Godbole et al. [4] and Nathanson [6].

Suppose $\Omega = \mathcal{A}_{n,m}$, and as before, denote a typical element of $\mathcal{A}_{n,m}$ by

$$\alpha(z) = z^{\beta_1} + \cdots + z^{\beta_m}.$$

Recall from Section 2 that $X := c_1^2 + \cdots + c_{n-1}^2 - \binom{m}{2}$ is a nonnegative-integer-valued random variable on Ω that attains the value 0 if and only if $\{\beta_1, \ldots, \beta_m\}$ is a Sidon set.

We have

$$\begin{aligned}
\mathbf{E}_{\mathcal{A}_{n,m}}(X) &= \mathbf{E}_{\mathcal{A}_{n,m}}(c_1^2 + \cdots + c_{n-1}^2) - \binom{m}{2} \\
&= \begin{cases} \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n)}{2n^{[4]}} & \text{if } n \text{ is even,} \\ \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n^2-2n+1)}{2n^{[4]}} & \text{if } n \text{ is odd} \end{cases} \\
&\leq \frac{m^{[4]}}{3(n-3)} + \frac{m^{[3]}(n-m)(n-1)^2}{2n^{[4]}} \\
&= \frac{m(m-1)(m-2)(2mn - 3n - m)}{6n(n-2)} \\
&\leq \frac{m^4}{3n}
\end{aligned}$$

if $n \geq 4$. On the other hand, if we let $B(n, m)$ be the number of Sidon sets in $[n]$ with m elements, then we have

$$\begin{aligned}
\mathbf{E}(X) = \frac{1}{\binom{n}{m}} \sum_{\alpha \in \mathcal{A}_{n,m}} X = \frac{1}{\binom{n}{m}} \sum_{\alpha \in \mathcal{A}_{n,m}, X>0} X \geq \frac{1}{\binom{n}{m}} \#\{\alpha \in \mathcal{A}_{n,m} : X(\alpha) > 0\} \\
\geq 1 - \frac{1}{\binom{n}{m}} B(n, m).
\end{aligned}$$

Hence we have proved (by essentially using Markov's inequality) the following.

https://doi.org/10.4153/CMB-2008-050-2 Published online by Cambridge University Press

Corollary 5.1 *For $4 \le m \le n$, we have*

$$B(n,m) \ge \binom{n}{m}\Big(1 - \frac{m^4}{3n}\Big)$$

and

$$\mathbf{Pr}[\{\beta_1,\dots,\beta_m\} \text{ is Sidon}] > 1 - \frac{m^4}{3n}.$$

Hence if $m = o(n^{1/4})$, then as n approaches infinity, the probability that a randomly chosen m-subset of $[n]$ is Sidon approaches 1.

Although when $m = o(n^{1/4})$, the probability that a randomly chosen m-subset of $[n]$ is Sidon approaches 1 (*i.e.*, $\|\alpha\|_4^4$ is $2m^2 - m$ for almost all $\alpha \in \mathcal{A}_{n,m}$), there are some other cases in which a positive proportion of polynomials in $\mathcal{A}_{n,m}$ have very large L_4 norm.

For $\alpha \in \mathcal{A}_{n,m}$, since for $0 \le k \le n-1$, $c_k = \sum_{j=0}^{n-k-1} a_j a_{j+k}$, we have $c_0 = m$, and for $1 \le k \le n-1$, $|c_k| \le \min\{m-1, n-k\}$. Therefore, we have

$$\begin{aligned}\|\alpha\|_4^4 = c_0^2 + 2\sum_{k=1}^{n-1} c_k^2 &\le m^2 + 2\sum_{k=1}^{n-m+1}(m-1)^2 + 2\sum_{k=n-m+2}^{n-1}(n-k)^2\\ &= 2nm^2 - \frac{4}{3}m^3 + 4m^2 - 4nm + 2n - \frac{5}{3}m\\ &= 2(1+o(1))m^2\Big(n - \frac{2}{3}m\Big)\end{aligned}$$

if $n = o(m^2)$ as $m, n \to \infty$ and on the other hand, from (4.15) we have

$$\begin{aligned}\frac{2(1+o(1))m^4}{3n} \le \mathbf{E}_{\mathcal{A}_{n,m}}(\|\alpha\|_4^4) &= \frac{1}{\binom{n}{m}}\sum_{\alpha\in\mathcal{A}_{n,m}}\|\alpha\|_4^4\\ &= \frac{1}{\binom{n}{m}}\Big\{\sum_{\|\alpha\|_4^4 \le x}\|\alpha\|_4^4 + \sum_{\|\alpha\|_4^4 > x}\|\alpha\|_4^4\Big\}\\ &\le x + \frac{1}{\binom{n}{m}}\sum_{\|\alpha\|_4^4 > x}\|\alpha\|_4^4\\ &\le x + \frac{1}{\binom{n}{m}}\sum_{\|\alpha\|_4^4 > x} 2(1+o(1))m^2\Big(n - \frac{2}{3}m\Big).\end{aligned}$$

It then follows that for any $x < 2(1+o(1))m^4/(3n)$, we have

$$\frac{\#\{\alpha\in\mathcal{A}_{n,m} : \|\alpha\|_4^4 > x\}}{\binom{n}{m}} \ge \frac{2(1+o(1))m^4/(3n) - x}{2(1+o(1))m^2(n - 2m/3)}.$$

In particular, for any $\epsilon > 0$, if $m = c_1 n$ and $x = c_2 m^2 n$ for $0 < c_1 < 1$ and $0 < c_2 < 2(1-\epsilon)c_1^2/3$, we have

$$\frac{\#\{\alpha \in \mathcal{A}_{n,m} : \|\alpha\|_4^4 > c_2 m^2 n\}}{\binom{n}{m}} \geq \frac{2(1-\epsilon)c_1^2/3 - c_2}{2(1+\epsilon)(1-2c_1/3)} > 0$$

for sufficiently large n and m, *i.e.,* there is a positive proportion of polynomials in $\mathcal{A}_{n,m}$ having large L_4 norm (note that the L_4 norm in $\mathcal{A}_{n,m}$ is at most as large as $2(1 + o(1))m^2 n$).

References

[1] P. B. Borwein, *Computational Excursions in Analysis and Number Theory.* CMS Books in Mathematics/Ouvrages de Mathmatiques de la SMC 10. Springer-Verlag, New York, 2002.

[2] P. B. Borwein and K.-K. S. Choi, *The average norm of polynomials of fixed height.* Trans. Amer. Math. Soc. **359**(2007), no. 2, 923–936.

[3] P. Erdős, *Some unsolved problems.* Michigan Math. J. **4**(1957), 291–300.

[4] A. P. Godbole, S. Janson, N. W. Locantore, Jr., and R. Rapoport, *Random Sidon sequences.* J. Number Theory **75**(1999), no. 1, 7–22.

[5] J. E. Littlewood, *Some Problems in Real and Complex Analysis.* D.C. Heath, Lexington, MA, 1968.

[6] M. B. Nathanson. *On the ubiquity of Sidon sets.* In: Number Theory. Springer, New York, 2004, pp. 263–272.

[7] D. J. Newman and J. S. Byrnes, *The L^4 norm of a polynomial with coefficients* ± 1. Amer. Math. Monthly **97**(1990), 42–45.

Department of Mathematics, Simon Fraser University, Burnaby, BC, V5A 1S6
e-mail: pborwein@cecm.sfu.ca
kkchoi@cecm.sfu.ca

Department of Mathematics, Atkinson Faculty, York University, Toronto, ON, M3J 1P3
e-mail: idmercer@yorku.ca