ON RANDOM BINARY SEQUENCES

KAI-UWE SCHMIDT

Abstract. A binary sequence $A = (a_0, a_1, \dots, a_{n-1})$ of length n is an element of $\{-1, 1\}^n$ and its autocorrelation at shift u is $C_u(A) = \sum_j a_j a_{j+u}$. We use the ℓ_r norm of $(C_1(A), C_2(A), \dots, C_{n-1}(A))$ to measure the collective smallness of the autocorrelations and, when A is drawn uniformly from $\{-1, 1\}^n$, determine the asymptotic behaviour, as $n \to \infty$, of the expectation of these norms and prove asymptotic concentration around the expected value. For integral r, we also give exact expressions for the expectation of the rth power of these ℓ_r norms. This complements results of Borwein and Lockhart for $r = 2$ and the present author for $r = \infty$ and extends partial results of Mercer for even integral r.

1. Introduction

Let $A = (a_0, a_1, \dots, a_{n-1})$ be an element of $\{-1, 1\}^n$, which we call a *binary sequence* of length n. The *aperiodic autocorrelation* of A at shift u is defined to be

$$C_u(A) = \sum_{j=0}^{n-u-1} a_j a_{j+u}.$$

There is sustained interest in binary sequences whose aperiodic autocorrelations at all nonzero shifts are small in magnitude relative to their lengths (see Turyn [17] and Jedwab [7] for excellent surveys). The numbers $C_u(A)$ are also related to several old unsolved problems concerning the behaviour on the unit circle of the polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$ (see Littlewood [9], [10, Problem 19], Erdős [5, Problem 22], [6], and Borwein [2] for surveys). This relationship arises since

$$\big|A(e^{i\theta})\big|^2 = n + 2\sum_{u=1}^{n-1} C_u(A)\cos(u\theta) \quad \text{for } \theta \in \mathbb{R}. \tag{1}$$

Let $x = (x_1, x_2, \dots, x_k)$ be an element of $\mathbb{R}^k$. For real $r > 0$, we write

$$\|x\|_r = \big(|x_1|^r + |x_2|^r + \cdots + |x_k|^r\big)^{1/r}.$$

This defines the ℓ_r norm in $\mathbb{R}^k$ for $r \geq 1$. We also define the ℓ_∞ *norm*

$$\|x\|_\infty = \max\big\{|x_1|, |x_2|, \dots, |x_k|\big\},$$

which equals the limit of $\|x\|_r$ as $r \to \infty$. For the binary sequence A write

$$C(A) = \big(C_1(A), C_2(A), \dots, C_{n-1}(A)\big).$$

Date: 25 March 2012.

K.-U. Schmidt was with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is now with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: kaiuwe.schmidt@ovgu.de.

The author is supported by German Research Foundation.

Then $\|C(A)\|_r$ measures the collective smallness of the aperiodic autocorrelations of A. In the sequence literature, $\|C(A)\|_\infty$ is called the *peak sidelobe level* of A and $\frac{1}{2}\,n^2/\|C(A)\|_2^2$ is called the *merit factor* of A.

Now let A_n be drawn uniformly from $\{-1,1\}^n$. In other words, each of the n sequence elements of A_n takes each of the values -1 and 1 independently with probability 1/2. We are interested in the asymptotic behaviour of the random variable $\|C(A_n)\|_r$. Recall that a sequence of random variables X_n *converges in probability* to a constant c if $\Pr(|X_n - c| \ge \epsilon) \to 0$ as $n \to \infty$ for all $\epsilon > 0$.

For the ℓ_∞ norm, the following result, proved by the author in [16], gives a complete solution to a problem due to Moon and Moser [12].

Theorem 1. [16, Theorem 1] *Let A_n be drawn uniformly from $\{-1,1\}^n$. Then, as $n \to \infty$,*

$$\frac{\|C(A_n)\|_\infty}{\sqrt{n\log n}} \to \sqrt{2} \quad \textit{in probability}$$

and

$$\frac{\mathrm{E}\left(\|C(A_n)\|_\infty\right)}{\sqrt{n\log n}} \to \sqrt{2}.$$

In this paper, we prove the following complementary result on $\|C(A_n)\|_r$ for finite r, in which $\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\,dt$ denotes the gamma function, satisfying $\Gamma(p+1) = p!$ when p is a nonnegative integer.

Theorem 2. *Let A_n be drawn uniformly from $\{-1,1\}^n$ and let r be a real number satisfying $0 < r < \infty$. Then, as $n \to \infty$,*

$$\frac{\|C(A_n)\|_r}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r} \quad \textit{in probability.} \tag{2}$$

and

$$\frac{\mathrm{E}(\|C(A_n)\|_r^r)}{n^{r/2+1}} \to \frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)} \tag{3}$$

Moreover, for $r \ge 1$, as $n \to \infty$,

$$\frac{\mathrm{E}(\|C(A_n)\|_r)}{n^{1/2+1/r}} \to \left(\frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+2)}\right)^{1/r}. \tag{4}$$

It is of significant interest to find the asymptotic behaviour of the minimum values of $\|C(A_n)\|_r$. Theorems 1 and 2 provide upper bounds for these minima. For $r = \infty$, nothing stronger is known and for $r = 2$, the best known result [8], obtained by binary sequences B_n formed by the Legendre symbol, is $\|C(B_n)\|_2/n \to c$, where $c < 25/89$ is strictly smaller than $1/\sqrt{2}$.

For $r = 2$, assertions (2) and (3) of Theorem 2 follow from [3, Theorem 1] by Borwein and Lockhart, which deals with norms of random polynomials. The relationship arises from the fact that, when the binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n is represented as a polynomial $A(z) = \sum_{j=0}^{n-1} a_j z^j$, then from (1),

$$n^2 + 2\,\|C(A)\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi} \left|A(e^{i\theta})\right|^4 d\theta.$$

Sarwate [15], and independently Newman and Byrnes [13], established the exact, rather than asymptotic, value of $\mathrm{E}(\|C(A_n)\|_2^2)$ to be $n(n-1)/2$. Assertion (3) of Theorem 2 was proved by Mercer [11, p. 669] when r is an even positive integer.

In fact, it was shown in [11, Theorem 1.4] that, in this case, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial in n, which can be easily computed using a recurrence relation. The key to this is the following elementary, but very useful, result, which was formally proved by Mercer [11, Proposition 1.1].

Proposition 3. *Let $X_0, X_1, \ldots, X_{n-1}$ be mutually independent random variables, each taking each of the values -1 and 1 with probability $1/2$. Then, for fixed $u \in \{1, 2, \ldots, n-1\}$, the $n-u$ products X_0X_u, $X_1, X_{1+u}, \ldots, X_{n-u-1}X_{n-1}$ are mutually independent.*

It is an immediate consequence of Proposition 3 that $C_{n-k}(A_n)$ is a transformed binomial random variable with parameters k and $1/2$. Hence, for $k \in \{1, 2, \ldots, n-1\}$ and real $r \geq 0$, the absolute moments $\mathrm{E}(|C_{n-k}(A_n)|^r)$ are given by

$$\frac{1}{2^{k-1}} \sum_{j<k/2} (k-2j)^r \binom{k}{j}. \tag{5}$$

When $r \geq 2$ is an even integer, Mercer [11, Theorem 1.4], building on a technique due to Romanovsky [14], gave a nice recurrence relation for the numbers (5). This shows that, when r is an even positive integer, (5) is a polynomial of degree $r/2$ in k, and therefore, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial of degree $r/2+1$ in n. Proposition 9 of this paper contains a recurrence relation for the numbers (5) for all real $r \geq 2$. This result together with an evaluation of (5) for $r = 1$ then shows that, when r is an odd positive integer, then

$$\frac{4^n}{\binom{2n}{n}} \mathrm{E}(\|C(A_{2n})\|_r^r) \quad \text{and} \quad \frac{4^n}{\binom{2n}{n}} \mathrm{E}(\|C(A_{2n+1})\|_r^r)$$

are polynomials of degree $(r+3)/2$ in n. This method enables us to derive exact, rather than asymptotic, values of $\mathrm{E}(\|C(A_n)\|_r^r)$ for odd integral $r \geq 1$.

2. Moments of autocorrelations

Let A_n be drawn uniformly from $\{-1, 1\}^n$. In this section we establish the asymptotic behaviour of the moments of the random vector $\big(C_u(A_n), C_v(A_n)\big)$, which will be the key to prove Theorem 2. We follow the method developed in [16]. Fix n and write $A_n = (a_0, a_1, \ldots, a_{n-1})$. Then, for nonnegative integers p and q, not both of them zero, we have

$$\begin{aligned} &\mathrm{E}\left(C_u(A_n)^p C_v(A_n)^q\right) \\ &\qquad = \sum_{i_1,\ldots,i_p=0}^{n-u-1} \sum_{j_1,\ldots,j_q=0}^{n-v-1} \mathrm{E}\left[a_{i_1}a_{i_1+u}\cdots a_{i_p}a_{i_p+u}a_{j_1}a_{j_1+v}\cdots a_{j_q}a_{j_q+v}\right]. \end{aligned} \tag{6}$$

Since the a_j's are mutually independent, $\mathrm{E}(a_j) = 0$, and $a_j^2 = 1$ for all $j \in \{0, 1, \ldots, n-1\}$, the expectation in the sum equals either zero or one. In particular, the expectation is nonzero exactly when the indices of the sequence elements occurring in the expectation match in pairs, so that it remains to count the number of cases when this happens. To do so, we define the notion of an even tuple as follows.

Definition 4. A tuple $(x_1, x_2, \ldots, x_k)$ is *even* if k is even and there exists a permutation σ of $\{1, 2, \ldots, k\}$ such that $x_{\sigma(2i-1)} = x_{\sigma(2i)}$ for each $i \in \{1, 2, \ldots, k/2\}$.

For example, $(1,3,1,4,3,4)$ is even, while $(2,1,1,2,1,3)$ is not even. In the following two lemmas we prove two results about even tuples. Recall that, for positive integer k, the double factorial

$$(2k-1)!! = \frac{(2k)!}{k!\,2^k} = (2k-1)(2k-3)\cdots 3\cdot 1$$

is the number of ways to arrange $2k$ objects into k unordered pairs.

Lemma 5. *Let m and k be positive integers and let R be the set of even tuples in*

$$\big\{(x_1,x_2,\dots,x_{2k}) : x_i\in\mathbb{Z},\, 0\le x_i<m\big\}.$$

Then

$$(2k-1)!!\,m(m-1)\cdots(m-k+1) \le |R| \le (2k-1)!!\,m^k.$$

Proof. There are $(2k-1)!!$ ways to arrange $x_1,x_2,\dots,x_{2k}$ into k unordered pairs. There are $m(m-1)\cdots(m-k+1)$ choices for k distinct values in $\{0,1,\dots,m-1\}$, which we assign to these pairs. In this way, we construct $(2k-1)!!\,m(m-1)\cdots(m-k+1)$ distinct even tuples in R, giving the lower bound. On the other hand, there are m^k choices for k values in $\{0,1,\dots,m-1\}$. In this way, we construct $(2k-1)!!\,m^k$ (not necessarily distinct) even tuples, which cover all elements of R. This gives the upper bound. □

Lemma 6. *Let u, v, and n be integers satisfying $0<u<v<n$. Let S be the set of all even tuples in $\{0,1,\dots,n-1\}^{2p+2q}$ of the form*

$$(x_1,x_1+u,\dots,x_p,x_p+u,y_1,y_1+v,\dots,y_q,y_q+v),$$

such that $(x_1,x_2,\dots,x_p)$ and $(y_1,y_2,\dots,y_q)$ are not both even. Then

$$|S| \le (2p+2q-1)!!\,(n-u)^{p/2}(n-v)^{(q-1)/2}.$$

Proof. Arrange the $2p+2q$ variables

$$x_1,x_1+u,\dots,x_p,x_p+u,y_1,y_1+v,\dots,y_q,y_q+v \tag{7}$$

into $p+q$ unordered pairs $(a_1,b_1),(a_2,b_2),\dots,(a_{p+q},b_{p+q})$ such that there are either fewer than $p/2$ pairs of the form (x_i,x_j) or fewer than $q/2$ pairs of the form (y_i,y_j). This can be done in at most $(2p+2q-1)!!$ ways. We formally set $a_i=b_i$ for all $i\in\{1,2,\dots,p+q\}$. If this assignment does not yield a contradiction, then we call the arrangement of (7) into $p+q$ pairs *consistent*. For example, if there are pairs of the form (x_i,y_j) and (x_i+u,y_j+v), then the arrangement is not consistent since $u\ne v$ by assumption.

Now, for every consistent arrangement, pairs of the form (x_i,x_j) or (y_i,y_j) determine the value of another pair (namely, (x_i+u,x_j+u) or (y_i+v,y_j+v), respectively). On the other hand, for every consistent arrangement, pairs not of the form

$$(x_i,x_j),\ (y_i,y_j),\ (x_i+u,x_j+u),\ \text{or } (y_i+v,y_j+v)$$

determine the value of at least two other pairs. For example, if there exists the pair (x_i,y_j), then x_i+u and y_j+v must lie in different pairs. Therefore, since there are either fewer than $p/2$ pairs of the form (x_i,x_j) or fewer than $q/2$ pairs of the form (y_i,y_j), for each consistent arrangement, at most $(p+q-1)/2$ of the variables $x_1,\dots,x_p,y_1,\dots,y_q$ can be chosen independently. Hence, since $u<v$, we can construct a set of at most $(2p+2q-1)!!\,(n-u)^{p/2}\,(n-v)^{(q-1)/2}$ tuples that contains S as a subset, as required. □

We now use Lemmas 5 and 6 to estimate the moments (6). We shall normalise the aperiodic autocorrelations of a binary sequence A of length n by defining

$$Y_u(A) = \frac{C_u(A)}{\sqrt{n-u}} \quad \text{for } u \in \{0, 1, \ldots, n-1\}. \tag{8}$$

Let Z be a standard normal random variable (which has zero mean and unit variance). By the definition of the Gamma function, we find that for real $r > -1$,

$$\mathrm{E}(|Z|^r) = \sqrt{\frac{2}{\pi}} \int_0^\infty x^r e^{-x^2/2}\, dx = \frac{2^{r/2}}{\sqrt{\pi}} \Gamma\Big(\frac{r+1}{2}\Big) = \frac{\Gamma(r+1)}{2^{r/2}\,\Gamma(r/2+1)}, \tag{9}$$

so that, since $\Gamma(p+1) = p!$ for nonnegative integral p and Z is symmetric, the moments of Z are

$$\mathrm{E}(Z^p) = \begin{cases} (p-1)!! & \text{for even } p \\ 0 & \text{for odd } p. \end{cases} \tag{10}$$

Proposition 7. *Let A_n be drawn uniformly from $\{-1, 1\}^n$. Let $g(n)$ be such that $1/g(n) \to 0$ as $n \to \infty$, and let Z be a standard normal random variable. Then, for nonnegative integers p and q,*

$$\lim_{n\to\infty} \max_{1 \le u < v \le n - g(n)} \Big| \mathrm{E}\left(Y_u(A_n)^p Y_v(A_n)^q\right) - \mathrm{E}(Z^p)\,\mathrm{E}(Z^q) \Big| = 0.$$

Proof. We may assume that p and q are not both zero. Let n be large enough, so that we can choose integers u and v such that $1 \le u < v \le n - g(n)$. Let T be the set of even tuples in $\{0, 1, \ldots, n-1\}^{2p+2q}$ of the form

$$(x_1, x_1 + u, \ldots, x_p, x_p + u, y_1, y_1 + v, \ldots, y_q, y_q + v).$$

Then, from (6) and (8),

$$\mathrm{E}\left(Y_u(A_n)^p Y_v(A_n)^q\right) = \frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}}.$$

First, assume that at least one of p and q is odd. Then, by Lemma 6,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}} \le \frac{(2p+2q-1)!!}{g(n)^{1/2}}$$

using $n - v \ge g(n)$. Since either $\mathrm{E}(Z^p) = 0$ or $\mathrm{E}(Z^q) = 0$ and the right hand side tends to zero as $n \to \infty$, the lemma is true when at least one of p or q is odd.

Now assume that p and q are both even. Then by Lemmas 5 and 6,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}} \le (p-1)!!\,(q-1)!! + \frac{(2p+2q-1)!!}{g(n)^{1/2}},$$

and by Lemma 5,

$$\frac{|T|}{(n-u)^{p/2}(n-v)^{q/2}} \ge (p-1)!!\,(q-1)!! \prod_{j=1}^{p/2-1} \left(1 - \frac{j}{g(n)}\right) \prod_{\ell=1}^{q/2-1} \left(1 - \frac{\ell}{g(n)}\right).$$

Hence, since $1/g(n) \to 0$, we conclude from (10) that the lemma is true when p and q are both even. □

We now use Proposition 7 to prove the following result on absolute moments.

Theorem 8. *Let A_n be drawn uniformly from $\{-1,1\}^n$. Let $g(n)$ be such that $1/g(n) \to 0$ as $n \to \infty$, and let Z be a standard normal random variable. Then, for real r and s satisfying $0 \le r, s < \infty$,*

$$\lim_{n\to\infty} \max_{1\le u<v\le n-g(n)} \Big| \mathrm{E}(|Y_u(A_n)|^r |Y_v(A_n)|^s) - \mathrm{E}(|Z|^r)\,\mathrm{E}(|Z|^s) \Big| = 0.$$

Before we prove the theorem, we recall some standard concepts from analysis (see [4] or [1] for a detailed treatment). A sequence of random elements $(X_{n,1},\dots,X_{n,m})$ in $\mathbb{R}^m$ with distribution function F_n *converges in distribution* to a random element $(X_1,\dots,X_m)$ in $\mathbb{R}^m$ with distribution function F if F_n converges pointwise to F at all points where F is continuous. The Continuous Mapping Theorem states that if $f : \mathbb{R}^m \to \mathbb{R}^k$ is continuous and $(X_{n,1},\dots,X_{n,m})$ converges in distribution to $(X_1,\dots,X_m)$, then $f(X_{n,1},\dots,X_{n,m})$ converges in distribution to $f(X_1,\dots,X_m)$ [1, Theorem 29.2].

A sufficient condition for convergence in distribution of $(X_{n,1},\dots,X_{n,m})$ to $(X_1,\dots,X_m)$ is that the distribution of $(X_1,\dots,X_m)$ is uniquely determined by the moments $\mathrm{E}(X_1^{p_1}\cdots X_m^{p_m})$ and $\mathrm{E}(X_{n,1}^{p_1}\cdots X_{n,m}^{p_m}) \to \mathrm{E}(X_1^{p_1}\cdots X_m^{p_m})$ for all nonnegative integers $p_1,\dots,p_m$ [1, Exercise 30.6]. We note that the distribution of an m-dimensional standard normal random variable (which has zero mean vector and identity covariance matrix) is uniquely determined by its moments [1, Exercise 30.5].

We shall make use of the following version of the Dominated Convergence Theorem. Let U_n and V_n be random variables satisfying $0 \le U_n \le V_n$ so that U_n converges in distribution to U and V_n converges in distribution to V. Then, if $\mathrm{E}(V_n) \to \mathrm{E}(V) < \infty$, then $\mathrm{E}(U_n) \to \mathrm{E}(U)$ (this is an extension of [4, Section 4.5, Exercise 2], in which $V_n = V$ for all n).

Proof of Theorem 8. Write $(Y_u(A_n), Y_v(A_n))$ in a triangular array such that the nth row contains $(Y_u(A_n), Y_v(A_n))$ for u, v satisfying $1 \le u < v \le n - g(n)$ in some arbitrary order. Construct a sequence of random elements $(X_{k,1}, X_{k,2})$ by reading out the rows of this array. Let Z_1 and Z_2 be independent standard normal random variables. Then Proposition 7 is equivalent to

$$\mathrm{E}(X_{k,1}^p X_{k,2}^q) \to \mathrm{E}(Z_1^p Z_2^q) \text{ as } k \to \infty, \text{ for all nonnegative integers } p \text{ and } q. \tag{11}$$

Now choose integers a and b such that $r \le 2a$ and $s \le 2b$. We apply the Dominated Convergence Theorem with

$$U_k = |X_{k,1}|^r\,|X_{k,2}|^s$$

and

$$V_k = (1+|X_{k,1}|^{2a})(1+|X_{k,2}|^{2b}),$$

so that $0 \le U_k \le V_k$ for all k. By (11) and the discussion preceding this proof, $(X_{k,1}, X_{k,2})$ converges in distribution to (Z_1, Z_2). By the Continuous Mapping Theorem, U_k converges in distribution to $U = |Z_1|^r\,|Z_2|^s$ and V_k converges in distribution to $V = (1+|Z_1|^{2a})(1+|Z_2|^{2b})$. By (11), $\mathrm{E}(V_k) \to \mathrm{E}(V)$, and therefore by the Dominated Convergence Theorem, $\mathrm{E}(|X_{k,1}|^r\,|X_{k,2}|^s) \to \mathrm{E}(|Z_1|^r|Z_2|^s)$, which is equivalent to the statement in the theorem. □

3. Proof of Theorem 2

We first prove assertion (3). Let $n > 2$ and $g(n)$ be the largest integer not greater than $\log n$. We use the normalisation (8) of $C_u(A_n)$ to write $\mathrm{E}(\|C(A_n)\|_r^r) = G_1(n) + G_2(n)$, where

$$G_1(n) = \sum_{u=1}^{g(n)-1} u^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)|^r),$$
$$G_2(n) = \sum_{u=g(n)}^{n-1} u^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)|^r).$$

The trivial bound $|Y_{n-u}(A_n)| \le u^{1/2}$ gives $|G_1(n)| < g(n)^{r+1}$, and therefore since $g(n) \le \log n$, the term $G_1(n)/n^{r/2+1}$ tends to zero as $n \to \infty$. Letting Z be a standard normal random variable, we have by Theorem 8 with $r = 0$ or $s = 0$,

$$\lim_{n\to\infty} \frac{G_2(n)}{n^{r/2+1}} = \mathrm{E}(|Z|^r) \lim_{n\to\infty} \frac{1}{n^{r/2+1}} \sum_{u=g(n)}^{n-1} u^{r/2} = \frac{\mathrm{E}(|Z|^r)}{r/2+1}.$$

The last step can be established by Riemann integration. Then, assertion (3) of the theorem follows from (9) and $z\,\Gamma(z) = \Gamma(z+1)$.

To prove assertion (2) of the theorem, we show with the same technique that

$$\frac{\mathrm{E}(\|C(A_n)\|_r^{2r})}{n^{r+2}} \to \left(\frac{\mathrm{E}(|Z|^r)}{r/2+1}\right)^2. \tag{12}$$

We have

$$\mathrm{E}(\|C(A_n)\|_r^{2r}) = \sum_{u=1}^{n-1}\sum_{v=1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r)$$
$$= \sum_{u=1}^{n-1} u^r\,\mathrm{E}(|Y_{n-u}(A_n)|^{2r}) + 2\sum_{u=1}^{n-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\,\mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r).$$

Proceeding as in the proof of assertion (3), we conclude that the first sum divided by n^{r+2} is $O(n^{-1})$, and therefore tends to zero as $n \to \infty$. We partition the second sum into $H_1(n)$ and $H_2(n)$, where

$$H_1(n) = 2\sum_{u=1}^{g(n)-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r),$$
$$H_2(n) = 2\sum_{u=g(n)}^{n-1}\sum_{v=u+1}^{n-1} (uv)^{r/2}\ \mathrm{E}(|Y_{n-u}(A_n)Y_{n-v}(A_n)|^r).$$

Since $|Y_{n-u}(A_n)Y_{n-v}(A_n)| \le (uv)^{1/2}$ and $g(n) \le \log n$, we have

$$\frac{|H_1(n)|}{n^{r+2}} < \frac{2}{n}(\log n)^{r+1}.$$

From Theorem 8 with $r = s$ we find that

$$\begin{aligned}\lim_{n\to\infty}\frac{H_2(n)}{n^{r+2}} &= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty}\frac{2}{n^{r+2}}\sum_{u=g(n)}^{n-1}\sum_{v=u+1}^{n-1}(uv)^{r/2}\\ &= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty}\frac{1}{n^{r+2}}\left(\sum_{u=g(n)}^{n-1}\sum_{v=g(n)}^{n-1}(uv)^{r/2} - \sum_{u=g(n)}^{n-1}u^r\right)\\ &= \big(\mathrm{E}(|Z|^r)\big)^2 \lim_{n\to\infty}\left(\frac{1}{n^{r/2+1}}\sum_{u=g(n)}^{n-1}u^{r/2}\right)^2\\ &= \left(\frac{\mathrm{E}(|Z|^r)}{r/2+1}\right)^2,\end{aligned}$$

which again can be established by Riemann integration. This proves our claim (12). Therefore, the variance of $\|C(A_n)\|_r^r/n^{r/2+1}$ tends to zero and assertion (2) follows from Chebyshev's inequality and the Continuous Mapping Theorem.

Now notice that convergence in probability to a constant c implies convergence in distribution to c. Assertion (4) of the theorem then follows from the inequality

$$\frac{\|C(A_n)\|_r}{n^{1/2+1/r}} \le 1 + \frac{\|C(A_n)\|_r^r}{n^{r/2+1}} \quad \text{for } r \ge 1$$

and the Dominated Convergence Theorem. □

4. Exact formulas for expected values

As before, we draw A_n uniformly from $\{-1,1\}^n$. In this section, we prove a recurrence relation for the moments of $C_u(A_n)$ from which the values $\mathrm{E}(\|C(A_n)\|_r^r)$ can be computed exactly when r is a positive integer.

Let $X_1, X_2, \ldots$ be mutually independent identically distributed random variables with $\Pr(X_1 = -1) = \Pr(X_1 = 1) = 1/2$ and define the random variable

$$S_k = \sum_{j=1}^{k} X_j.$$

Then, by Proposition 3, $C_{n-k}(A_n)$ and S_k have the same distribution for $k \in \{1,2,\ldots,n-1\}$, and hence for real $r \ge 0$,

$$\mathrm{E}(\|C(A_n)\|_r^r) = \sum_{k=1}^{n-1}\mathrm{E}(|S_k|^r). \tag{13}$$

We are therefore interested in the values $\mathrm{E}(|S_k|^r)$, for which we have the following recurrence relation.

Proposition 9. *For integral $k \ge 0$ and real $r \ge 2$, we have*

$$\mathrm{E}(|S_k|^r) = k^2\ \mathrm{E}(|S_k|^{r-2}) - k(k-1)\ \mathrm{E}(|S_{k-2}|^{r-2}).$$

Proof. Recall that

$$\mathrm{E}(|S_k|^r) = \frac{1}{2^{k-1}}\sum_{j<k/2}(k-2j)^r\binom{k}{j}. \tag{14}$$

We have

$$\begin{aligned}(k-2j)^2\binom{k}{j} &= k^2\binom{k}{j} - 4j(k-j)\binom{k}{j}\\ &= k^2\binom{k}{j} - 4k(k-1)\binom{k-2}{j-1}.\end{aligned}$$

Substitution into (14) gives

$$\mathrm{E}(|S_k|^r) = \frac{k^2}{2^{k-1}}\sum_{j<k/2}(k-2j)^{r-2}\binom{k}{j} - \frac{k(k-1)}{2^{k-3}}\sum_{j<k/2-1}(k-2-2j)^{r-2}\binom{k-2}{j},$$

from which the required recurrence follows by using (14) again. □

Mercer [11, Theorem 1.4] gave a proof of Proposition 9 when r is an even positive integer by inspecting the moment generating function of S_k. In this case, the initial condition for the recurrence is $\mathrm{E}(|S_k|^0) = 1$, and we get for example,

$$\begin{aligned}\mathrm{E}(|S_k|^2) &= k,\\ \mathrm{E}(|S_k|^4) &= 3k^2 - 2k,\end{aligned}$$

and therefore by (13),

$$\begin{aligned}\mathrm{E}(\|C(A_n)\|_2^2) &= \tfrac{1}{2}(n^2-n),\\ \mathrm{E}(\|C(A_n)\|_4^4) &= \tfrac{1}{2}(2n^3-5n^2+3n).\end{aligned}$$

In general, when r is an even positive integer, $\mathrm{E}(|S_k|^r)$ is a polynomial of degree $r/2$ in k, and therefore, $\mathrm{E}(\|C(A_n)\|_r^r)$ is a polynomial of degree $r/2+1$ in n.

To apply Proposition 9 when r is an odd positive integer, we require the following result, which is number A.4 of the 1974 Putnam competition. The proof, which is an evaluation of (14) for $r = 1$, is left to the reader.

Lemma 10. *For positive integral k,*

$$\mathrm{E}(|S_k|) = \frac{1}{2^{k-1}}\binom{k}{\lceil k/2\rceil}\left\lceil\frac{k}{2}\right\rceil.$$

By straightforward manipulations, we can rewrite the recurrence relation of Proposition 9 as

$$\mathrm{E}(|S_k|^r) = \frac{1}{2^{k-1}}\binom{k}{\lceil k/2\rceil}\left\lceil\frac{k}{2}\right\rceil F_r(k),$$

where $F_r(k)$ satisfies, for integral $k \geq 0$ and real $r \geq 2$,

$$F_r(k) = k^2F_{r-2}(k) - 4\lfloor k/2\rfloor(\lceil k/2\rceil - 1)F_{r-2}(k-2).$$

Now let r be an odd positive integer. Then, since $F_1(k) = 1$ by Lemma 10, $F_r(2k)$ and $F_r(2k+1)$ are polynomials of degree $(r-1)/2$ in k. For example,

$$\begin{aligned}F_3(2k) &= 4k, & F_3(2k+1) &= 4k+1,\\ F_5(2k) &= 32k^2-16k, & F_5(2k+1) &= 32k^2+8k+1.\end{aligned}$$

Notice that we can rewrite $\mathrm{E}(|S_{2k+1}|^r)$ in terms of $\binom{2k}{k}$ using

$$\binom{2k+1}{k+1} = \frac{2k+1}{k+1}\binom{2k}{k}.$$

Then, separating the sum in (13) into sums over even and odd k, we get

$$\mathrm{E}(\|C(A_n)\|_r^r) = \sum_{k<n/2} \frac{2k\,F_r(2k)}{4^k}\binom{2k}{k} + \sum_{k<(n-1)/2} \frac{(2k+1)F_r(2k+1)}{4^k}\binom{2k}{k}.$$

It remains to evaluate

$$\lambda_t(n) = \sum_{k=0}^{n-1} \frac{k^t}{4^k}\binom{2k}{k}$$

for integral $t \geq 0$. By telescoping, we find that

$$\lambda_0(n) = \sum_{k=0}^{n-1}\left[\frac{2(k+1)}{4^{k+1}}\binom{2k+2}{k+1} - \frac{2k}{4^k}\binom{2k}{k}\right] = \binom{2n}{n}\frac{2n}{4^n}.$$

When $t > 0$, the sums $\lambda_t(n)$ can then be evaluated via reduction, viz

$$\lambda_t(n) = \sum_{m=1}^{n-1}\sum_{k=0}^{n-1} \frac{k^{t-1}}{4^k}\binom{2k}{k} - \sum_{m=1}^{n-1}\sum_{k=0}^{m-1} \frac{k^{t-1}}{4^k}\binom{2k}{k}.$$

For example,

$$\lambda_1(n) = \binom{2n}{n}\frac{2n(n-1)}{3\cdot 4^n},$$
$$\lambda_2(n) = \binom{2n}{n}\frac{2n(n-1)(3n-1)}{15\cdot 4^n}$$

(the expression for $\lambda_1(n)$ is a solution to Problem E 995 in the December 1951 issue of the American Mathematical Monthly). We then get, for example,

$$\mathrm{E}(\|C(A_{2n})\|_1) = \binom{2n}{n}\frac{8n^2-2n}{3\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n+1})\|_1) = \binom{2n}{n}\frac{8n^2+4n}{3\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n})\|_3^3) = \binom{2n}{n}\frac{96n^3-68n^2+2n}{15\cdot 4^n},$$
$$\mathrm{E}(\|C(A_{2n+1})\|_3^3) = \binom{2n}{n}\frac{96n^3+52n^2+2n}{15\cdot 4^n}.$$

In general, when r is an odd positive integer,

$$\frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n})\|_r^r) \quad \text{and} \quad \frac{4^n}{\binom{2n}{n}}\,\mathrm{E}(\|C(A_{2n+1})\|_r^r)$$

are polynomials of degree $(r+3)/2$ in n.

Acknowledgement

I wish to thank Richard Lockhart for very helpful discussions on the subject of this paper.

References

1. P. Billingsley, *Probability and measure*, 3rd ed., John Wiley & Sons, Inc., 1995.
2. P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics, Springer-Verlag, New York, NY, 2002.
3. P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, Proc. Amer. Math. Soc. **129** (2001), no. 5, 1463–1472.
4. K. L. Chung, *A course in probability theory*, Harcourt, Brace & World, Inc., 1968.
5. P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.
6. ———, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.
7. J. Jedwab, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.
8. J. Jedwab, D. J. Katz, and K.-U. Schmidt, *Littlewood polynomials with small L^4 norm*, preprint (2011).
9. 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.
10. ———, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
11. I. D. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), no. 5, 663–671.
12. J. W. Moon and L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), no. 12, 340–343.
13. D. J. Newman and J. S. Byrnes, *The L^4 norm of a polynomial with coeffiecients ± 1*, Amer. Math. Monthly **97** (1990), no. 1, 42–45.
14. V. Romanovsky, *Note on the moments of a binomial $(p+q)^n$ about its mean*, Biometrika **15** (1923), no. 3/4, 410–412.
15. D. V. Sarwate, *Mean-square correlation of shift-register sequences*, IEE Proc. **131, Part F** (1984), no. 2, 101–106.
16. K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, arXiv:1105.5178 [math.CO] (2011).
17. R. J. Turyn, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968.