THE PEAK SIDELOBE LEVEL OF RANDOM BINARY SEQUENCES

KAI-UWE SCHMIDT

Abstract. Let $A_n = (a_0, a_1, \dots, a_{n-1})$ be drawn uniformly at random from $\{-1,+1\}^n$ and define

$$M(A_n) = \max_{0<u<n} \left| \sum_{j=0}^{n-u-1} a_j a_{j+u} \right| \quad \text{for } n > 1.$$

It is proved that $M(A_n)/\sqrt{n \log n}$ converges in probability to $\sqrt{2}$. This settles a problem first studied by Moon and Moser in the 1960s and proves in the affirmative a recent conjecture due to Alon, Litsyn, and Shpunt. It is also shown that the expectation of $M(A_n)/\sqrt{n \log n}$ tends to $\sqrt{2}$.

1. Introduction

Consider a binary sequence $A = (a_0, a_1, \dots, a_{n-1})$ of length n, namely an element of $\{-1,+1\}^n$. Define the *aperiodic autocorrelation* at shift u of A to be

$$C_u(A) = \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } u \in \{0, 1, \dots, n-1\}$$

and define the *peak sidelobe level* of A as

$$M(A) = \max_{0<u<n} |C_u(A)| \quad \text{for } n > 1.$$

Binary sequences with small autocorrelation at nonzero shifts have a wide range of applications in digital communications, including synchronisation and radar (see [6], for example).

Let $\mu(n)$ be the minimum of $M(A)$ taken over all 2^n binary sequences A of length n. By a parity argument, it is seen that $\mu(n) \geq 1$ and it is known that $\mu(n) = 1$ for $n \in \{2, 3, 4, 5, 7, 11, 13\}$ (binary sequences attaining the minimum are often called *Barker* sequences). It is a classical problem to decide whether $\mu(n) > 1$ for all $n > 13$. Although deep methods have been developed [14], [13], this problem is still open; the currently smallest undecided case arises for $n > 2 \cdot 10^{30}$ [8]. It is conjectured that $\mu(n)$ grows

---

Date: 21 February 2011 (revised 21 December 2013).

2010 *Mathematics Subject Classification.* Primary: 05D40; Secondary: 94A55, 60F10.

The author was supported by German Research Foundation under Research Fellowship SCHM 2609/1-1.

as $n \to \infty$, perhaps like $\sqrt{n}$. We refer to Turyn [15] and Jedwab [7] for excellent surveys on this problem.

In this paper, we will be concerned with the asymptotic behaviour, as $n \to \infty$, of $M(A)$ for almost all binary sequences A of length n. This problem was first studied by Moon and Moser [12]. Let A_n be a random binary sequence of length n, by which we mean that A_n is drawn uniformly at random from $\{-1,+1\}^n$. In other words, each of the n sequence elements of A_n takes on each of the values -1 and $+1$ independently with probability $1/2$. Until now, the best known bounds are

$$\lim_{n\to\infty} \Pr\left[1-\epsilon < \frac{M(A_n)}{\sqrt{n\log n}} < \sqrt{2}+\epsilon\right] = 1 \quad \text{for all } \epsilon > 0. \tag{1.1}$$

The upper bound is due to Mercer [11]. In fact, Mercer proved a weaker result but pointed out in a final remark [11, p. 670] that his proof establishes the above upper bound. The lower bound was proved by Alon, Litsyn, and Shpunt [2], in response to numerical evidence provided by Dmitriev and Jedwab [4]. The authors of [2] also conjectured that the lower bound can be improved to $\sqrt{2}-\epsilon$. The aim of this paper is to prove this conjecture and therefore to establish the limit distribution, as $n \to \infty$, of $M(A_n)/\sqrt{n\log n}$. In particular, we prove the following.

Theorem 1.1. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

$$\frac{M(A_n)}{\sqrt{n\log n}} \to \sqrt{2} \quad \textit{in probability}$$

and

$$\frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} \to \sqrt{2}.$$

Alon, Litsyn, and Shpunt [2] already observed that, as a consequence of McDiarmid's inequality (Lemma 3.1), $M(A_n)$ is concentrated around its expected value, but could only show that

$$\liminf_{n\to\infty} \frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} \ge 1. \tag{1.2}$$

Their proof considers $C_u(A_n)$ only for $u \ge n/2$ and crucially relies on the fact that $C_u(A_n)$ and $C_v(A_n)$ are independent whenever $n/2 \le u < v < n$. Our method considers $C_u(A_n)$ also for $u < n/2$. In particular, by a careful estimation of the moments of $C_u(A_n)C_v(A_n)$ for $0 < u < v < n$, we will show that the lower bound (1.2) can be improved to $\sqrt{2}$, which together with (1.1) establishes the second part of Theorem 1.1. The first part of Theorem 1.1 then follows from McDiarmid's inequality.

As pointed out in [2], given a binary sequence $A = (a_0, a_1, \dots, a_{n-1})$ of length n, the quantity $M(A)$ is related to the more general rth-order correlation measure $S_r(A)$, which was defined by Mauduit and Sárközy [9] to be

$$S_r(A) := \max_{0\le u_1<u_2<\cdots<u_r<n} \max_{0\le k\le n-u_r} \left| \sum_{j=0}^{k-1} a_{j+u_1}a_{j+u_2}\cdots a_{j+u_r} \right| \quad \text{for } n \ge r.$$

Alon, Kohayakawa, Mauduit, Moreira, and Rödl [1] established that, given a random binary sequence A_n of length n, then for all $r \ge 2$,

$$\lim_{n\to\infty} \Pr\left[\frac{2}{5} < \frac{S_r(A_n)}{\sqrt{n\log\binom{n}{r}}} < \sqrt{3}+\epsilon\right] = 1 \quad \text{for all } \epsilon > 0.$$

Since, for every binary sequence A, we have $M(A) \le S_2(A)$, Theorem 1.1 implies that for $r = 2$ the lower bound can be improved from $2/5$ to $1-\epsilon$.

2. Preliminary Results

The main results of this section are the following. Given a random binary sequence A_n of length n, Proposition 2.2 gives a lower bound for

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \tag{2.1}$$

for small u. This result can also be concluded from [2]. However, the proof presented here is considerably simpler and more direct. Proposition 2.7 gives an upper bound for

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n} \cap |C_v(A_n)| \ge \sqrt{2n\log n}\right] \tag{2.2}$$

for $0 < u < v < n$. These bounds will be the crucial ingredients to prove the main result of this paper.

2.1. To bound (2.1), we shall need the following refinement of the central limit theorem.

Lemma 2.1 (Cramér [3, Thm. 2])**.** *Let $X_0, X_1, \ldots$ be identically distributed mutually independent random variables satisfying $\mathrm{E}[X_0] = 0$ and $\mathrm{E}[X_0^2] = 1$ and suppose that there exists $T > 0$ such that $\mathrm{E}[e^{tX_0}] < \infty$ for all $|t| < T$. Write $Y_k = X_0 + X_1 + \cdots + X_{k-1}$ and let Φ be the distribution function of a normal random variable with zero mean and unit variance. If $\theta_k > 1$ and $\theta_k/k^{1/6} \to 0$ as $k \to \infty$, then*

$$\frac{\Pr\left[|Y_k| \ge \theta_k\sqrt{k}\right]}{2\Phi(-\theta_k)} \to 1.$$

Proposition 2.2. *Let A_n be a random binary sequence of length $n > 2$ and let u be an integer satisfying $1 \le u \le \frac{n}{\log n}$. Then*

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \ge \frac{1}{5n\sqrt{\log n}}$$

for all sufficiently large n.

Proof. Write $A_n = (a_0, a_1, \dots, a_{n-1})$. It is well known that the $n-u$ products

$$a_0a_u,\ a_1a_{1+u}, \dots, a_{n-u-1}a_{n-1}$$

are mutually independent. A proof of this fact was given by Mercer [11, Prop. 1.1]. Hence $C_u(A_n)$ is a sum of $n-u$ mutually independent random variables, each taking each of the values -1 and $+1$ with probability $1/2$. Notice that $\mathrm{E}[e^{ta_0a_u}] = \cosh(t)$ and, setting

$$\xi_n = \sqrt{\frac{2n\log n}{n-u}},$$

we find that $\xi_n/(n-u)^{1/6} \to 0$ since $u \le \frac{n}{\log n}$. We can therefore apply Lemma 2.1 to conclude, as $n \to \infty$,

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \sim 2\Phi(-\xi_n), \tag{2.3}$$

where Φ is the distribution function of a standard normal random variable. It is well known (see [5, Thm. 1.2.3], for example) that

$$\frac{1}{\sqrt{2\pi}\,z}\left(1-\frac{1}{z^2}\right)e^{-z^2/2} \le \Phi(-z) \le \frac{1}{\sqrt{2\pi}\,z}\,e^{-z^2/2} \quad \text{for } z>0,$$

so that, since $\frac{n}{n-u} \sim 1$, as $n \to \infty$,

$$2\Phi(-\xi_n) \sim \frac{1}{\sqrt{\pi\log n}}\,e^{-\frac{n}{n-u}\log n}.$$

Using $u \le \frac{n}{\log n}$, we conclude

$$e^{-\frac{n}{n-u}\log n} \ge e^{-\frac{\log n}{\log n-1}\,\log n} \sim \frac{1}{en}$$

as $n \to \infty$. It then follows from (2.3) that for all $\alpha > e\sqrt{\pi}$ and all sufficiently large n we have

$$\Pr\left[|C_u(A_n)| \ge \sqrt{2n\log n}\right] \ge \frac{1}{\alpha n\sqrt{\log n}}.$$

The lemma follows since $5 > e\sqrt{\pi}$. ☐

2.2. We now turn to the derivation of an upper bound for (2.2). It will be convenient to define the notion of an even tuple as follows.

Definition 2.3. A tuple $(x_1, x_2, \dots, x_{2m})$ is *even* if there exists a permutation σ of $\{1, 2, \dots, 2m\}$ such that $x_{\sigma(2i-1)} = x_{\sigma(2i)}$ for each $i \in \{1, 2, \dots, m\}$.

For example, $(1, 3, 1, 4, 3, 4)$ is even, while $(2, 1, 1, 2, 1, 3)$ is not even. In the next two lemmas we will prove two results about even tuples, which we then use to estimate moments of $C_u(A_n)C_v(A_n)$.

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 2.4. *Let m and q be positive integers and let R be the set of even tuples in*

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

Then

$$|R| \le (2q-1)!!\, m^q.$$

Proof. There are $(2q-1)!!$ ways to arrange $x_1, x_2, \dots, x_{2q}$ into q unordered pairs and to each of these q pairs we assign a value of $\{0, 1, \dots, m-1\}$. In this way we construct all elements of R at least once, which proves the lemma. □

Lemma 2.5. *Let u, v, and n be integers satisfying $0 < u, v < n$ and $u \ne v$. Write $I = \{1, 2, \dots, 2q\}$ and let t be an integer satisfying $0 \le t < q$. Let S be the subset of*

$$\big\{(x_i, x_i + u, y_i, y_i + v)_{i \in I} \,:\, x_i, y_i \in \mathbb{Z},\, 0 \le x_i < n - u,\, 0 \le y_i < n - v\big\}$$

containing all even elements $(x_i, x_i + u, y_i, y_i + v)_{i \in I}$ such that $(x_i)_{i \in J}$ is not even for all $(2q - 2t)$-element subsets J of I. Then

$$|S| \le (8q-1)!!\, n^{2q-(t+1)/3}.$$

Proof. We will construct a set of tuples that contains S as a subset. Arrange the $8q$ variables

$$x_1, x_1 + u, \dots, x_{2q}, x_{2q} + u, y_1, y_1 + v, \dots, y_{2q}, y_{2q} + v \tag{2.4}$$

into $4q$ unordered pairs $(a_1, b_1), (a_2, b_2), \dots, (a_{4q}, b_{4q})$ such that there are at most $q - t - 1$ pairs (x_i, x_j). This can be done in at most $(8q-1)!!$ ways. We formally set $a_i = b_i$ for all $i \in \{1, 2, \dots, 4q\}$. If this assignment does not yield a contradiction, then we call the arrangement of (2.4) into $4q$ 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 at most $q - t - 1$ pairs of the form (x_i, x_j) and at most q pairs of the form (y_i, y_j), for each consistent arrangement, at most

$$\tfrac{1}{2}(4q - 2t - 2) + \tfrac{1}{3}(2t + 2) = 2q - \tfrac{1}{3}(t + 1)$$

of the variables $x_1, \dots, x_{2q}, y_1, \dots, y_{2q}$ can be chosen independently. We assign to each of these a value of $\{0, 1, \dots, n-1\}$. In this way, we construct a set of at most $(8q-1)!!\, n^{2q-(t+1)/3}$ tuples that contains S as a subset, as required. □

We now use Lemmas 2.4 and 2.5 to bound moments of $C_u(A_n)C_v(A_n)$.

Lemma 2.6. *Let p and h be integers satisfying $0 \le h < p$ and let A_n be a random binary sequence of length n. Then, for $0 < u < v < n$,*

$$\mathrm{E}\Big[\big(C_u(A_n)C_v(A_n)\big)^{2p}\Big] \le n^{2p}\big[(2p-1)!!\big]^2\left(1+\frac{(8p)^{8h}}{n^{1/3}}+\frac{(8p)^{4p}}{n^{(h+1)/3}}\right).$$

Proof. Write $I = \{1, 2, \dots, 2p\}$ and let T be the set containing all even tuples of

$$\big\{(x_i, x_i+u, y_i, y_i+v)_{i\in I} \,:\, x_i, y_i \in \mathbb{Z},\; 0 \le x_i < n-u,\; 0 \le y_i < n-v\big\}.$$

Writing $A_n = (a_0, a_1, \dots, a_{n-1})$, we have

$$\begin{aligned}
&\mathrm{E}\Big[\big(C_u(A_n)C_v(A_n)\big)^{2p}\Big]\\
&= \mathrm{E}\left[\bigg(\sum_{i=0}^{n-u-1} a_i a_{i+u}\bigg)^{2p}\bigg(\sum_{j=0}^{n-v-1} a_j a_{j+v}\bigg)^{2p}\right]\\
&= \sum_{i_1,\dots,i_{2p}=0}^{n-u-1}\;\sum_{j_1,\dots,j_{2p}=0}^{n-v-1} \mathrm{E}\left[a_{i_1}a_{i_1+u}\cdots a_{i_{2p}}a_{i_{2p}+u}a_{j_1}a_{j_1+v}\cdots a_{j_{2p}}a_{j_{2p}+v}\right]\\
&= |T| \qquad (2.5)
\end{aligned}$$

since $a_0, a_1, \dots, a_{n-1}$ are mutually independent, $\mathrm{E}[a_j] = 0$, and $a_j^2 = 1$ for all $j \in \{0, 1, \dots, n-1\}$. We define the following subsets of T.

(1) T_1 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ are even.
(2) T_2 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that $(x_i)_{i\in I}$ or $(y_i)_{i\in I}$ is not even and $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even for some $(2p-2h)$-element subsets J and K of I.
(3) T_3 contains all elements $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ of T such that either $(x_i)_{i\in J}$ is not even for all $(2p-2h)$-element subsets J of I or $(y_i)_{i\in K}$ is not even for all $(2p-2h)$-element subsets K of I.

It is immediate that T_1, T_2, and T_3 partition T, so that

$$|T| = |T_1| + |T_2| + |T_3|. \qquad (2.6)$$

We now bound the cardinalities of T_1, T_2, and T_3.

The set T_1. Using Lemma 2.4, we have the crude estimate

$$|T_1| \le \big[(2p-1)!!\big]^2 n^{2p}. \qquad (2.7)$$

The set T_2. Let $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ be an element of T_2. Then there exist $(2p-2h)$-element subsets J and K of I such that $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even and

$$(x_i)_{i\in I\setminus J} \quad \text{or} \quad (y_i)_{i\in I\setminus K} \qquad (2.8)$$

is not even. Since $(x_i)_{i\in J}$ and $(y_i)_{i\in K}$ are even, $(x_i, x_i+u, y_j, y_j+v)_{i\in J,\, j\in K}$ is even. Since $(x_i, x_i+u, y_i, y_i+v)_{i\in I}$ is also even, it follows that

$$(x_i, x_i+u, y_j, y_j+v)_{i\in I\setminus J,\, j\in I\setminus K} \tag{2.9}$$

is even as well. There are $\binom{2p}{2h}$ subsets J and $\binom{2p}{2h}$ subsets K. By Lemma 2.4, for each such J and K, there are at most $(2p-2h-1)!!\,n^{p-h}$ even tuples $(x_i)_{i\in J}$ satisfying $0 \le x_i < n$ for each $i \in J$ and at most $(2p-2h-1)!!\,n^{p-h}$ even tuples $(y_i)_{i\in K}$ satisfying $0 \le y_i < n$ for each $i \in K$. By Lemma 2.5 applied with $t = 0$ and by interchanging u and v and $(x_i)_{i\in I\setminus J}$ and $(y_i)_{i\in I\setminus K}$ if necessary, the number of even tuples in $\{0, 1, \dots, n-1\}^{8h}$ of the form (2.9) such that one of the tuples in (2.8) is not even is at most $(8h-1)!!\,n^{2h-1/3}$. Therefore,

$$\begin{aligned} |T_2| &\le 2n^{2h-1/3}\,(8h-1)!!\left[\binom{2p}{2h}(2p-2h-1)!!\,n^{p-h}\right]^2 \\ &\le n^{2p-1/3}\big[(2p-1)!!\big]^2\,(8p)^{8h}, \end{aligned} \tag{2.10}$$

using very crude bounds.

The set T_3. By Lemma 2.5 applied with $t = h$ and by interchanging u and v and $(x_i)_{i\in I}$ and $(y_i)_{i\in I}$ if necessary,

$$\begin{aligned} |T_3| &\le 2n^{2p-(h+1)/3}\,(8p-1)!! \\ &\le n^{2p-(h+1)/3}\,(8p)^{4p}. \end{aligned} \tag{2.11}$$

Now the lemma follows by combining (2.5), (2.6), (2.7), (2.10), and (2.11). □

Lemma 2.6 is now used to prove the desired upper bound for (2.2).

Proposition 2.7. *Let A_n be a random binary sequence of length n and write $\lambda_n = \sqrt{2n\log n}$. Then, for $0 < u < v < n$ and all sufficiently large n,*

$$\Pr\big[|C_u(A_n)| \ge \lambda_n \,\cap\, |C_v(A_n)| \ge \lambda_n\big] \le \frac{23}{n^2}.$$

Proof. Let (X_1, X_2) be a random vector taking values in $\mathbb{R}\times\mathbb{R}$ and let p be a positive integer. Then by Markov's inequality, for $\theta_1, \theta_2 > 0$,

$$\Pr\big[|X_1| \ge \theta_1 \,\cap\, |X_2| \ge \theta_2\big] \le \frac{\mathrm{E}\big[(X_1X_2)^{2p}\big]}{(\theta_1\theta_2)^{2p}}.$$

Let h be an arbitrary integer satisfying $0 \le h < p$. Application of Lemma 2.6 gives

$$\begin{aligned} &\Pr\big[|C_u(A_n)| \ge \lambda_n \,\cap\, |C_v(A_n)| \ge \lambda_n\big) \\ &\qquad\le \frac{\big[(2p-1)!!\big]^2}{(2\log n)^{2p}}\big[1 + K_1(n,p,h) + K_2(n,p,h)\big], \end{aligned} \tag{2.12}$$

where

$$K_1(n,p,h)=n^{-1/3}\,(8p)^{8h}\quad\text{and}\quad K_2(n,p,h)=n^{-(h+1)/3}\,(8p)^{4p}.$$

We apply (2.12) with $p=\lfloor\log n\rfloor$ and $h=\lfloor 17\log\log n\rfloor$, so that for all sufficiently large n we have $h<p$, as assumed. By Stirling's approximation

$$\sqrt{2\pi k}\;k^ke^{-k}\le k!\le\sqrt{3\pi k}\;k^ke^{-k},$$

we have

$$\frac{\big[(2p-1)!!\big]^2}{(2\log n)^{2p}}\le\frac{3p^{2p}e^{-2p}}{(\log n)^{2p}}\le\frac{3e^2}{n^2}.$$

We also have

$$\begin{aligned}K_1(n,p,h)&\le K_1(n,\log n,17\log\log n)\\&=n^{-\frac{1}{3}}n^{\frac{136(\log\log n)(\log 8+\log\log n)}{\log n}}\\&=O(n^{-1/4})\quad\text{as }n\to\infty\end{aligned}$$

and

$$\begin{aligned}K_2(n,p,h)&\le K_2(n,\log n,16\log\log n)\\&=n^{-\frac{1}{3}+4\log 8-\frac{4}{3}\log\log n}\\&=O(n^{-\log\log n})\quad\text{as }n\to\infty.\end{aligned}$$

Substitute into (2.12) to obtain the claimed result, using $3e^2<23$. □

3. Proof of Main Theorem

We require the following result, which is a consequence of Azuma's inequality for martingales.

Lemma 3.1 (McDiarmid [10]). *Let $X_0,X_1,\dots,X_{n-1}$ be mutually independent random variables taking values in a set S. Let $f:S^n\to\mathbb{R}$ be a measurable function and suppose that f satisfies*

$$\big|f(x)-f(y)\big|\le c$$

whenever x and y differ only in one coordinate. Define the random variable $Y=f(X_0,X_1,\dots,X_{n-1})$. Then, for $\theta\ge 0$,

$$\Pr\Big[\big|Y-\mathrm{E}[Y]\big|\ge\theta\Big]\le 2e^{-\frac{2\theta^2}{c^2n}}.$$

Given a random binary sequence $A_n=(a_0,a_1,\dots,a_{n-1})$ of length n, we will apply Lemma 3.1 with $X_j=a_j$ for $j\in\{0,1,\dots,n-1\}$ and

$$f(x_0,x_1,\dots,x_{n-1})=\max_{0<u<n}\left|\sum_{j=0}^{n-u-1}x_jx_{j+u}\right|,$$

so that $M(A_n)=f(a_0,a_1,\dots,a_{n-1})$. We can take $c=4$ in Lemma 3.1 and obtain the following corollary.

Corollary 3.2. *Let A_n be a random binary sequence of length n. Then, for $\theta \geq 0$,*

$$\Pr\left[\left|M(A_n) - \mathrm{E}[M(A_n)]\right| \geq \theta\right] \leq 2e^{-\frac{\theta^2}{8n}}.$$

We now prove the second part of Theorem 1.1.

Theorem 3.3. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

$$\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} \to \sqrt{2}.$$

Proof. By the triangle inequality and the union bound we have, for all $\epsilon > 0$,

$$\Pr\left[\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} - \sqrt{2} > \epsilon\right]$$
$$\leq \Pr\left[\frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} - \frac{M(A_n)}{\sqrt{n \log n}} > \tfrac{1}{2}\epsilon\right] + \Pr\left[\frac{M(A_n)}{\sqrt{n \log n}} - \sqrt{2} > \tfrac{1}{2}\epsilon\right].$$

By Corollary 3.2 and the upper bound of (1.1), the two terms on the right-hand side tend to zero as $n \to \infty$, hence

$$\limsup_{n\to\infty} \frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} \leq \sqrt{2}. \tag{3.1}$$

Let $\delta > 0$ and define the set

$$N(\delta) = \left\{n > 1 : \frac{\mathrm{E}\left[M(A_n)\right]}{\sqrt{n \log n}} < \sqrt{2} - \delta\right\}. \tag{3.2}$$

We claim that the size of $N(\delta)$ is finite for all choices of δ, which together with (3.1) will prove the theorem. The proof of the claim is based on an idea developed in [2]. Let $n > 2$ and write

$$W = \left\{u \in \mathbb{Z} : 1 \leq u \leq \frac{n}{\log n}\right\}$$

and $\lambda_n = \sqrt{2n \log n}$. Then

$$\Pr\left[M(A_n) \geq \lambda_n\right] \geq \Pr\left[\max_{u\in W} |C_u(A_n)| \geq \lambda_n\right]$$
$$\geq \sum_{u\in W} \Pr\left[|C_u(A_n)| \geq \lambda_n\right] - \sum_{\substack{u,v\in W\\ u<v}} \Pr\left[|C_u(A_n)| \geq \lambda_n \cap |C_v(A_n)| \geq \lambda_n\right]$$

by the Bonferroni inequality. By Propositions 2.2 and 2.7,

$$\begin{aligned}\Pr\left[M(A_n) \geq \lambda_n\right] &\geq |W| \cdot \frac{1}{5n(\log n)^{\frac{1}{2}}} - \frac{|W|^2}{2} \cdot \frac{23}{n^2}\\ &\geq \frac{1}{8(\log n)^{\frac{3}{2}}} - \frac{12}{(\log n)^2}\\ &\geq \frac{1}{10(\log n)^{\frac{3}{2}}} \qquad (3.3)\end{aligned}$$

for all sufficiently large n, using $\frac{2}{3}\frac{n}{\log n} \le |W| \le \frac{n}{\log n}$ for $n > 2$. Now, by the definition (3.2) of $N(\delta)$, for all $n \in N(\delta)$ we have $\lambda_n > \mathrm{E}[M(A_n)]$, so that we can apply Corollary 3.2 with $\theta = \lambda_n - \mathrm{E}[M(A_n)]$ to give, for all $n \in N(\delta)$,

$$\Pr\big[M(A_n) \ge \lambda_n\big] \le 2e^{-\frac{1}{8n}(\lambda_n - \mathrm{E}[M(A_n)])^2}.$$

Comparison with (3.3) yields, for all sufficiently large $n \in N(\delta)$,

$$\frac{1}{10(\log n)^{\frac{3}{2}}} \le 2e^{-\frac{1}{8n}(\lambda_n - \mathrm{E}[M(A_n)])^2},$$

which implies

$$\frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} \ge \sqrt{2} - \sqrt{\frac{12\log\log n + 8\log 20}{\log n}}.$$

From the definition (3.2) of $N(\delta)$ it then follows that $N(\delta)$ has finite size for all $\delta > 0$, as required. □

Using Corollary 3.2, it is now straightforward to prove the first part of Theorem 1.1.

Corollary 3.4. *Let A_n be a random binary sequence of length n. Then, as $n \to \infty$,*

$$\frac{M(A_n)}{\sqrt{n\log n}} \to \sqrt{2} \quad \textit{in probability.}$$

Proof. By the triangle inequality and the union bound we have, for all $\epsilon > 0$,

$$\Pr\left[\left|\frac{M(A_n)}{\sqrt{n\log n}} - \sqrt{2}\right| > \epsilon\right]$$
$$\le \Pr\left[\left|\frac{M(A_n)}{\sqrt{n\log n}} - \frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}}\right| > \tfrac{1}{2}\epsilon\right] + \Pr\left[\left|\frac{\mathrm{E}\big[M(A_n)\big]}{\sqrt{n\log n}} - \sqrt{2}\right| > \tfrac{1}{2}\epsilon\right].$$

By Corollary 3.2 and Theorem 3.3, the two terms on the right-hand side tend to zero as $n \to \infty$, which proves the corollary. □

Acknowledgement

I would like to thank Jonathan Jedwab for many valuable discussions and Jonathan Jedwab and Daniel J. Katz for their careful comments on this paper.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl, *Measures of pseudorandomness: Typical values*, Proc. Lond. Math. Soc **95** (2007), no. 3, 778–812.
[2] N. Alon, S. Litsyn, and A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inform. Theory **56** (2010), no. 1, 545–554.
[3] H. Cramér, *Sur un nouveau théorème-limite de la théorie des probabilités*, Actualités Sci. Indust. **736** (1938), 5–23.

[4] D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Adv. Math. Commun. **1** (2007), 461–475.
[5] R. Durrett, *Probability: Theory and examples*, 4th ed., Cambridge University Press, 2010.
[6] S. W. Golomb and G. Gong, *Signal design for good correlation: For wireless communication, cryptography, and radar*, Cambridge University Press, Cambridge, 2005.
[7] J. Jedwab, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.
[8] K. H. Leung and B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64** (2012), no. 1-2, 143–151.
[9] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), no. 4, 265–377.
[10] C. McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics (J. Siemons, ed.), London Math. Soc. Lectures Notes Ser. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188.
[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] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), no. 4, 929–952.
[14] R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), no. 1, 319–346.
[15] ———, *Sequences with small correlation*, Error Correcting Codes (Henry B. Mann, ed.), Wiley, New York, 1968.

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

Current address: Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany.

E-mail address: `kaiuwe.schmidt@ovgu.de`