Bounding the peak sidelobe level of binary sequences of all lengths

Idris Mercer
Florida International University
imercer@fiu.edu

Abstract

Improving upon 2010 results of Alon, Litsyn, and Shpunt, it was shown in 2014 by Schmidt that asymptotically, almost all binary sequences of length n have peak sidelobe level close to $\sqrt{2n \log n}$. One specific result of Alon, Litsyn, and Shpunt is that if we fix $\varepsilon > 0$, then almost all binary sequences of length n have peak sidelobe level at most $\sqrt{2n(\log n - (1.5 - \varepsilon) \log \log n)}$, in the sense that the probability of not satisfying that bound approaches 0 as n approaches infinity. In this note, we prove that for all sequence lengths $n > 1$, there is a binary sequence of length n with peak sidelobe level at most $\sqrt{2n(\log n - \log \log n + 0.862)}$.

By a **binary sequence** of **length** n, we mean an n-tuple

$$A = (a_0, a_1, \ldots, a_{n-1})$$

where each a_j is $+1$ or -1. For $0 \leq k \leq n-1$, we define the (acyclic or aperiodic) **autocorrelations** of A by

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

Informally, c_k measures how much the sequence A resembles a version of itself that has been shifted by k positions.

We let $\mathcal{B}_n$ denote the set of all 2^n binary sequences of length n. For any $A \in \mathcal{B}_n$, we have $c_0 = n$. We refer to $c_1, \ldots, c_{n-1}$ as the **nontrivial** autocorrelations of A. An old problem, arising in communications engineering but also of interest as a stand-alone combinatorial problem, involves trying to find binary sequences in $\mathcal{B}_n$ whose nontrivial autocorrelations are 'close' to zero in some sense.

For any $A \in \mathcal{B}_n$, we define the **peak sidelobe level** (PSL) of A by

$$\mu(A) = \max_{1 \le k \le n-1} |c_k| \,.$$

We consider A to be a 'good' sequence if $\mu(A)$ is small. If A is a constant sequence, then trivially $\mu(A) = n - 1$, but very informally speaking, if A is 'random' then $\mu(A)$ tends to be significantly smaller than $O(n)$. Many authors have investigated upper bounds for $\mu(A)$. (For an excellent survey, see [3].) We might try to find upper bounds for $\mu(A)$ that hold for some sequences $A \in \mathcal{B}_n$, or that hold for almost all sequences $A \in \mathcal{B}_n$.

To make this more precise, we turn $\mathcal{B}_n$ into a probability space by supposing the a_j are independent Rademacher variables (i.e., random variables each equally likely to be $+1$ or -1). This is equivalent to assigning equal weight to each of the 2^n sequences in $\mathcal{B}_n$, and for any function $f(n)$, the probability that $\mu(A) \le f(n)$ is equal to the proportion of sequences $A \in \mathcal{B}_n$ that satisfy $\mu(A) \le f(n)$. We say $\mu(A) \le f(n)$ for 'almost all' sequences $A \in \mathcal{B}_n$ if

$$\lim_{n \to \infty} \mathbf{Pr}\big[\mu(A) \le f(n)\big] = 1.$$

We also define

$$\mu_{\min}(n) = \min_{A \in \mathcal{B}_n} \mu(A)$$

so then if $\mu(A) \le f(n)$ for a nonzero proportion of sequences $A \in \mathcal{B}_n$, we have $\mu_{\min}(n) \le f(n)$.

In 2014, Schmidt proved [7] (improving upon previous results by Alon, Litsyn & Shpunt [1], the current author [4], and Moon & Moser [5]) that if we fix $\varepsilon > 0$, then the probability

$$\mathbf{Pr}\Big[(\sqrt{2} - \varepsilon)\sqrt{n \log n} \le \mu(A) \le (\sqrt{2} + \varepsilon)\sqrt{n \log n}\Big] \qquad (1)$$

approaches 1 as n approaches infinity (informally, almost all sequences $A \in \mathcal{B}_n$ have peak sidelobe level 'close' to $\sqrt{2n \log n}$). Here and throughout this article, 'log' means natural log.

Earlier, Schmidt [6] gave an explicit construction showing that for each $n > 1$, there is a sequence $A \in \mathcal{B}_n$ satisfying $\mu(A) \leq \sqrt{2n\log(2n)}$. He also gave numerical evidence for the conjecture that his sequences satisfy $\mu(A) = O(\sqrt{n \log\log n})$. As pointed out in [3], several authors have conjectured that there is an infinite family of binary sequences satisfying $\mu(A) = O(\sqrt{n})$, but this has not been proved. In fact, the best upper bounds that have been proved to hold *either* for a positive proportion of sequences *or* for almost all sequences appear to be of the form $\mu(A) = O(\sqrt{n \log n})$.

Because of the lower bound in (1), it is not possible to prove that almost all sequences $A \in \mathcal{B}_n$ satisfy an upper bound of the form $\mu(A) = o(\sqrt{n \log n})$. However, if $f(n)$ is a certain function of n that approaches infinity more slowly than $\log n$, it can be shown that almost all sequences $A \in \mathcal{B}_n$ satisfy $\mu(A) \leq \sqrt{2n(\log n - f(n))}$. One such result is Corollary 4.3 in [1], which shows that if we fix $\varepsilon > 0$, then the proportion of sequences $A \in \mathcal{B}_n$ satisfying

$$\mu(A) > \sqrt{2n(\log n - (1.5 - \varepsilon)\log\log n)}$$

is bounded above by a multiple of $1/(\log n)^{\varepsilon}$, and hence approaches 0 as n approaches infinity. That is, in an asymptotic sense, almost all binary sequences of length n satisfy

$$\mu(A) \leq \sqrt{2n(\log n - (1.5 - \varepsilon)\log\log n)}.$$

In this note, we prove the following, which is not as good in an asymptotic sense, but which holds for all lengths $n > 1$.

Proposition. *For all $n > 1$, the proportion of sequences $A \in \mathcal{B}_n$ satisfying*

$$\mu(A) > \sqrt{2n(\log n - \log\log n + 0.862)}$$

is strictly less than 1. It follows that for all $n > 1$, we have

$$\mu_{\min}(n) \leq \sqrt{2n(\log n - \log\log n + 0.862)}.$$

In the proof of the proposition, we will need the following elementary lemma.

Lemma. If $n > 1$ and K is a constant, then

$$\frac{K - \log\log n}{\log n} \geq \frac{-1}{e^{K+1}}.$$

Proof. Consider the function

$$f(x) = \frac{K - \log x}{x}$$

for $x > 0$. Using elementary calculus, we find

$$f'(x) = \frac{\log x - (K+1)}{x^2}$$

which is negative when $0 < x < e^{K+1}$ and positive when $x > e^{K+1}$. It follows that for all $x > 0$, we have

$$f(x) \geq f(e^{K+1}) = \frac{-1}{e^{K+1}}$$

and therefore for all $n > 1$, we have

$$\frac{K - \log\log n}{\log n} = f(\log n) \geq \frac{-1}{e^{K+1}}.$$

Proof of Proposition:

As mentioned before, we turn $\mathcal{B}_n$ into a probability space by supposing the a_j to be independent Rademacher variables, which is equivalent to assigning equal weight to all 2^n sequences in $\mathcal{B}_n$.

Note that the autocorrelation

$$c_k = a_0 a_k + a_1 a_{k+1} + \cdots + a_{n-k-1} a_{n-1}$$

is a sum of $n - k$ terms, each of which is ± 1. In fact, those $n - k$ terms are independent. (This is straightforward but not quite trivial; for a proof, see [4].) If $1 \leq k \leq n - 1$, then c_{n-k} is a sum of k independent Rademacher variables, so we can use Chernoff-type bounds (see, e.g., Corollary A.1.2 in Appendix A of [2]) to conclude that if $\lambda > 0$, then

$$\mathbf{Pr}\big[\, |c_{n-k}| > \lambda \big] < 2\exp(-\lambda^2/2k).$$

Let $\lambda = \sqrt{2n\psi(n)}$, where we define

$$\psi(n) = \log n - \log\log n + 0.862.$$

We then have

$$\mathbf{Pr}\Big[\,|c_{n-k}| > \sqrt{2n\psi(n)}\Big] < 2\exp(-n\psi(n)/k).$$

We call a sequence $A \in \mathcal{B}_n$ 'good' if $\mu(A) \leq \sqrt{2n\psi(n)}$, and 'bad' otherwise. Then A is bad if and only if $|c_{n-k}| > \sqrt{2n\psi(n)}$ for some $k = 1, \ldots, n-1$. An overestimate for $\mathbf{Pr}[A \text{ is bad}]$ is

$$\sum_{k=1}^{n-1} \mathbf{Pr}\Big[\,|c_{n-k}| > \sqrt{2n\psi(n)}\Big] < \sum_{k=1}^{n-1} 2\exp(-n\psi(n)/k).$$

Now, consider the function

$$g(x) = 2\exp(-\psi(n)/x)$$

on the interval $x \in [\frac{1}{n}, 1]$. The function $g(x)$ is an increasing function of x on that interval, so a left-endpoint Riemann sum will be an underestimate for an integral:

$$\sum_{k=1}^{n-1} g\Big(\frac{k}{n}\Big)\frac{1}{n} < \int_{1/n}^{1} g(x)dx$$

$$\implies \sum_{k=1}^{n-1} g\Big(\frac{k}{n}\Big) < n\int_{1/n}^{1} g(x)dx$$

$$\implies \sum_{k=1}^{n-1} 2\exp(-n\psi(n)/k) < 2n\int_{1/n}^{1} \exp(-\psi(n)/x)dx$$

$$\implies \mathbf{Pr}[A \text{ is bad}] < 2n\int_{1/n}^{1} \exp(-\psi(n)/x)dx.$$

We will now perform the substitution $u = \psi(n)/x$ on this integral. We have

$$\begin{aligned}
u &= \psi(n)x^{-1} \\
du &= -\psi(n)x^{-2}dx \\
-\big(x^2/\psi(n)\big)du &= dx \\
x = 1/n \Rightarrow u &= n\psi(n) \\
x = 1 \Rightarrow u &= \psi(n) \\
x &= \psi(n)/u \\
x^2 &= \big(\psi(n)\big)^2/u^2 \\
x^2/\psi(n) &= \psi(n)/u^2 \\
dx = -\big(x^2/\psi(n)\big)du &= -\big(\psi(n)/u^2\big)du
\end{aligned}$$

and so the above integral becomes

$$\begin{aligned}
2n\int_{1/n}^{1} \exp(-\psi(n)/x)dx &= 2n\int_{n\psi(n)}^{\psi(n)} \exp(-u)\Big(-\frac{\psi(n)}{u^2}\Big)du \\
&= 2n\psi(n)\int_{\psi(n)}^{n\psi(n)} \frac{1}{u^2e^u}du.
\end{aligned}$$

That is, we have

$$\mathbf{Pr}[A \text{ is bad}] < 2n\psi(n)\int_{\psi(n)}^{n\psi(n)} \frac{1}{u^2e^u}du.$$

Now since the function $h(u) = 1/u^2e^u$ decreases very rapidly, a rather crude upper bound will suffice. We have

$$\int_{\psi(n)}^{n\psi(n)} \frac{1}{u^2e^u}du < \int_{\psi(n)}^{\infty} \frac{1}{u^2e^u}du.$$

On the interval $u \in (\psi(n), \infty)$, we have $u^2 > (\psi(n))^2$, so we have

$$\int_{\psi(n)}^{\infty} \frac{1}{u^2e^u}du < \frac{1}{(\psi(n))^2}\int_{\psi(n)}^{\infty} e^{-u}du = \frac{1}{(\psi(n))^2}e^{-\psi(n)}.$$

This implies that we have

$$\mathbf{Pr}[A \text{ is bad}] < 2n\psi(n) \cdot \frac{1}{(\psi(n))^2}e^{-\psi(n)} = \frac{2n}{\psi(n)e^{\psi(n)}}.$$

Now since $\psi(n) = \log n - \log\log n + 0.862$, we have

$$\begin{aligned} \exp\big(\psi(n)\big) &= \exp(\log n)\exp(-\log\log n)\exp(0.862) \\ &= n(\log n)^{-1}e^K \end{aligned}$$

where for brevity, we write $K = 0.862$. We then have

$$\begin{aligned} \psi(n)e^{\psi(n)} &= \big(\log n - \log\log n + K\big)\cdot n(\log n)^{-1}e^K \\ &= e^K\Big(1 + \frac{K - \log\log n}{\log n}\Big)n \end{aligned}$$

and then our lemma implies

$$\psi(n)e^{\psi(n)} \geq e^K\Big(1 + \frac{-1}{e^{K+1}}\Big)n = \Big(e^K - \frac{1}{e}\Big)n.$$

Now note that

$$e^K - \frac{1}{e} = e^{0.862} - \frac{1}{e} > 2.00001$$

so we have

$$\frac{2n}{\psi(n)e^{\psi(n)}} < \frac{2n}{2.00001n} = \frac{2}{2.00001} < 1$$

which completes the proof of the proposition.

References

[1] N. Alon, S. Litsyn & A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inform. Theory **56** (2010), 545–554.

[2] N. Alon & J.H. Spencer, *The Probabilistic Method* (3rd ed.) John Wiley & Sons, 2008.

[3] J. Jedwab & K. Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE Trans. Inform. Theory **52** (2006), 2247–2254.

[4] I.D. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), 663–671.

[5] J.W. Moon & L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), 340–343.

[6] K.-U. Schmidt, *Binary sequences with small peak sidelobe level*, IEEE Trans. Inform. Theory **58** (2012), 2512–2515.

[7] K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, Bull. Lond. Math. Soc. **46** (2014), 643–652.