BINARY SEQUENCES WITH SMALL PEAK SIDELOBE LEVEL

KAI-UWE SCHMIDT

ABSTRACT. A binary sequence of length $n$ is an $n$-tuple with elements in \{-1,1\} and its peak sidelobe level is the largest absolute value of its aperiodic autocorrelations at nonzero shifts. A classical problem is to find binary sequences whose peak sidelobe level is small compared to the length of the sequence. Using known techniques from probabilistic combinatorics, this paper gives a construction for a binary sequence of length $n$ with peak sidelobe level at most $\sqrt{2n\log(2n)}$ for every $n > 1$. This improves the best known bound for the peak sidelobe level of a family of explicitly constructed binary sequences, which arises for the family of $m$-sequences. By numerical analysis it is argued that the peak sidelobe level of the constructed sequences grows in fact like order $\sqrt{n \log \log n}$, and therefore grows strictly more slowly than the peak sidelobe level of a typical binary sequence.

1. Introduction

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a binary sequence of length $n > 1$, namely an element of \{-1,1\}$^n$. The aperiodic autocorrelation at shift $u$ of $A$ is given by

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

for $u \in \{0, 1, \ldots, n-1\}$.

A classical problem in digital sequence design is to find binary sequences whose aperiodic autocorrelations (at nonzero shifts) are small in magnitude (see [3], [21], [4], [5], [18], [11], [6], [15], for example, and [10] for a survey). Accordingly, we define the peak sidelobe level of $A$ to be

$$M(A) = \max_{0 < u < n} |C_u(A)|.$$

By a parity argument, $M(A) \geq 1$ for all binary sequences $A$ of length greater than 1. A Barker sequence is a binary sequence $B$ that satisfies $M(B) = 1$. Such sequences exist for lengths 2, 3, 4, 5, 7, 11, and 13. It has been conjectured since at least 1960 [19] that there is no Barker sequence of length greater than 13. This conjecture has been proved for odd lengths by Turyn and Storer [20] and for all even lengths up to $2 \cdot 10^{30}$ (see Leung and B. Schmidt [12] for most recent results).

Let $\mu(n)$ be the minimum of $M(A)$ taken over all binary sequences $A$ of length $n$. Then $\mu(n) = 1$ if and only if there is a Barker sequence of length $n$. The value $\mu(n)$ can be computed with an apparent time complexity of $O(1.4^n)$ [4]. Currently, $\mu(n)$
is known for all \( n \leq 61 \) and for \( n = 64 \) (see Coxson and Russo [5] for most recent results). Many authors have put considerable computational effort in finding binary sequences with small peak sidelobe level (see Nunn and Coxson [15], for example), showing that

\[
\mu(n) \leq 2 \quad \text{for each } n \leq 21,
\]
\[
\mu(n) \leq 3 \quad \text{for each } n \leq 48,
\]
\[
\mu(n) \leq 4 \quad \text{for each } n \leq 82,
\]
\[
\mu(n) \leq 5 \quad \text{for each } n \leq 105.
\]

Turyn conjectured [21, p. 198] that the infimum limit of \( \mu(n) \) is infinite. It has also been conjectured by several authors (see Jedwab [9] for historical background) that there exists a positive constant \( c \) such that, for all \( n > 1 \) and all binary sequences \( A \) of length \( n \),

\[
\sum_{u=1}^{n-1} (C_u(A))^2 \geq cn^2.
\]

This is known as the Merit Factor Conjecture and implies that \( \mu(n)/\sqrt{n} \) is bounded away from 0 as \( n \to \infty \). More specifically, based on a heuristic argument, Ein-Dor, Kanter, and Kinzel [7] conjectured that, as \( n \to \infty \),

\[
\frac{\mu(n)}{\sqrt{n}} \to d, \quad \text{where } d = 0.435 \ldots.
\]

Mercer [13] proved that the peak sidelobe level of a random binary sequence of length \( n \) is typically not significantly larger than \( \sqrt{2n \log n} \), thereby improving a result by Moon and Moser [14]. The author proved that the peak sidelobe level of a random binary sequence of length \( n \) is also typically not significantly smaller than \( \sqrt{2n \log n} \), which improves a result by Alon, Litsyn, and Shpunt [1].

**Theorem 1** (Schmidt [17]). Let \( A_n \) be drawn uniformly from \( \{-1,0,1\}^n \). Then, as \( n \to \infty \),

\[
\frac{M(A_n)}{\sqrt{n} \log n} \to \sqrt{2} \quad \text{in probability.}
\]

In view of Theorem 1, it is rather surprising that the currently strongest proven result for the peak sidelobe level of a specific family of binary sequences grows like order \( \sqrt{n \log n} \) as \( n \to \infty \). This result occurs for the family of \( m \)-sequences, which are binary sequences that exist for all lengths of the form \( 2^m - 1 \) (see Golomb and Gong [8], for example, for background on \( m \)-sequences).

**Theorem 2** (Sarwate [16]). Let \( Y \) be an \( m \)-sequence of length \( n = 2^m - 1 \). Then

\[
M(Y) \leq 1 + \frac{2}{\pi} \sqrt{n + 1} \log \left( \frac{4n}{\pi} \right).
\]

Using known techniques from probabilistic combinatorics, we give a construction for a binary sequence of length \( n \) with peak sidelobe level at most \( \sqrt{2n \log(2n)} \) for every \( n > 1 \). The construction is based on a derandomisation approach (see Alon and Spencer [2], for example) and can be implemented with \( O(n^2) \) additions and \( O(n^2) \) multiplications. By numerical analysis we argue that the peak sidelobe level of the constructed sequences grows like order \( \sqrt{n \log \log n} \) as \( n \to \infty \), and therefore grows strictly more slowly than the peak sidelobe level of a typical binary sequence.
2. Main Result

We begin with stating the promised construction.

**Construction 3.** Let \( n \) be a positive integer and write \( \theta = \sqrt{(2/n) \log(2n)} \). Construct a binary sequence \( B_n = (b_0, b_1, \ldots, b_{n-1}) \) of length \( n \) recursively by

\[
b_r = -\text{sign} \left( \sum_{u=1}^{r-1} b_{r-u} \sinh \left( \theta \sum_{j=0}^{r-u-1} b_j b_{j+u} \right) \right),
\]

where, by convention, \( \text{sign}(0) = 0 \).

Notice that we always have \( b_0 = b_1 = 1 \). The first few nontrivial binary sequences obtained under Construction 3 are

\[
B_3 = (1, 1, -1),
B_4 = (1, 1, -1, 1),
B_5 = (1, 1, -1, 1, 1),
B_6 = (1, 1, -1, 1, 1, 1),
B_7 = (1, 1, -1, 1, 1, 1, -1).
\]

The pattern may suggest that \( B_n \) is an initial segment of \( B_{n+1} \), which is however not the case in general.

The following theorem gives an upper bound on the peak sidelobe level of \( B_n \).

**Theorem 4.** The binary sequence \( B_n \) of length \( n > 1 \) obtained under Construction 3 satisfies

\[
M(B_n) \leq \sqrt{2n \log(2n)}.
\]

**Proof.** Fix an integer \( n > 1 \) and define, for \( r \in \{0, 1, \ldots, n\} \) and \( u \in \{1, 2, \ldots, n-1\} \), the function \( f_{u,r} : \{-1, 1\}^r \to \mathbb{R} \) by

\[
f_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \begin{cases} 
2e^{-\theta^2 n}(\cosh \theta)^{n-r} \cosh \left( \theta \sum_{j=0}^{r-u-1} x_j x_{j+u} \right) & \text{for } 0 < u \leq r - 1 \\
2e^{-\theta^2 n}(\cosh \theta)^{-u} & \text{for } r - 1 \leq u < n.
\end{cases}
\]

Notice that \( f_{r-1,r} \) is well defined. Let \( I[E] \) be the indicator of an event \( E \) (which equals 1 if \( E \) occurs and equals 0 otherwise), and let \( A = (a_0, a_1, \ldots, a_{n-1}) \) be an arbitrary binary sequence of length \( n \). Straightforward manipulation gives, for each \( u \in \{1, 2, \ldots, n-1\} \),

\[
I\left[|C_u(A)| > \sqrt{2n \log(2n)}\right] = I[C_u(A) > \theta n] + I[-C_u(A) > \theta n] = I[e^{\theta C_u(A)} > e^{\theta^2 n}] + I[e^{-\theta C_u(A)} > e^{\theta^2 n}] < e^{-\theta^2 n} \left( e^{\theta C_u(A)} + e^{-\theta C_u(A)} \right)
\]

\[
= f_{u,n}(a_0, a_1, \ldots, a_{n-1}).
\]

Write \( B_n = (b_0, b_1, \ldots, b_{n-1}) \). We claim that

\[
\sum_{u=1}^{n-1} f_{u,n}(b_0, b_1, \ldots, b_{n-1}) < 1,
\]
so that by (1),
\[ \sum_{u=1}^{n-1} I[|C_u(B_n)|] > \sqrt{2n \log(2n)} < 1. \]
Hence, all of the indicators are zero and therefore
\[ |C_u(B_n)| \leq \sqrt{2n \log(2n)} \quad \text{for each } u \in \{1, 2, \ldots, n-1\}, \]
proving the theorem.

It remains to prove the claim (2). We first show that, for \( u \in \{1, 2, \ldots, n-1\} \) and \( r \in \{0, 1, \ldots, n-1\} \), we have
\[ (3) \quad f_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \frac{1}{2} f_{u,r+1}(x_0, x_1, \ldots, x_{r-1}, 1) + \frac{1}{2} f_{u,r+1}(x_0, x_1, \ldots, x_{r-1}, -1). \]
This holds trivially for \( u \geq r \). For \( u < r \), we use
\[ \cosh(y + z) + \cosh(y - z) = 2 \cosh(z) \cosh(y) \]
to conclude
\[ \frac{1}{2} f_{u,r+1}(x_0, \ldots, x_{r-1}, 1) + \frac{1}{2} f_{u,r+1}(x_0, \ldots, x_{r-1}, -1) \]
\[ = 2e^{-\frac{\theta^2 n}{2}} (\cosh \theta)^{n-r-1} \cosh(\theta x_{r-u}) \cosh \left( \theta \sum_{j=0}^{r-u-1} x_j x_{j+u} \right) \]
\[ = f_{u,r}(x_0, x_1, \ldots, x_{r-1}) \]
since \( x_{r-u} \in \{-1, 1\} \) and \( \cosh \) is an even function.

Now, since \( \sinh \) is an odd function, we can rewrite \( b_r \) as
\[ b_r = -\text{sign} \left[ \sum_{u=1}^{r-1} 2 \sinh(\theta b_{r-u}) \sinh \left( \theta \sum_{j=0}^{r-u-1} b_j b_{j+u} \right) \right]. \]
Use
\[ 2 \sinh(z) \sinh(y) = \cosh(y + z) - \cosh(y - z) \]
to conclude that \( b_r \) is an \( x \in \{-1, 1\} \) that minimises
\[ \sum_{u=1}^{r-1} \cosh \left( \theta \sum_{j=0}^{r-u-1} b_j b_{j+u} + \theta b_{r-u} x \right). \]
We therefore find from (3) that
\[ (4) \quad \sum_{u=1}^{n-1} f_{u,r+1}(b_0, b_1, \ldots, b_r) \leq \sum_{u=1}^{n-1} f_{u,r}(b_0, b_1, \ldots, b_{r-1}) \]
for each \( r \in \{0, 1, \ldots, n-1\} \). Using \( \cosh x \leq e^{x^2/2} \), we have
\[ \sum_{u=1}^{n-1} f_{u,0} \leq \sum_{u=1}^{n-1} 2e^{-\frac{\theta^2 (n+u)/2}{2}} \]
\[ \leq 2(n-1)e^{-\frac{\theta^2 n}{2}} \]
\[ = 1 - \frac{1}{n} \]
since \( \theta^2 n = 2 \log(2n) \). The claim (2) then follows by combination with (4) and induction on \( r \). \( \square \)
3. Efficient Implementation

Fix an integer \( n > 1 \) and assume the notation used in Construction 3. Define, for \( r \in \{1, 2, \ldots, n\} \) and \( u \in \{1, 2, \ldots, r\} \), the functions \( c_{u,r}, s_{u,r} : \{-1,1\}^r \to \mathbb{R} \) by

\[
c_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \cosh \left( \theta \sum_{j=0}^{r-u-1} x_j x_{j+u} \right)
\]
\[
s_{u,r}(x_0, x_1, \ldots, x_{r-1}) = \sinh \left( \theta \sum_{j=0}^{r-u-1} x_j x_{j+u} \right).
\]

Assume that \( b_0, \ldots, b_{r-1} \) have been already determined. Since \( b_0 = b_1 = 1 \), we may also assume that \( r > 1 \). We wish to calculate \( s_{u,r}(b_0, \ldots, b_{r-2}) \) for \( u \in \{1, 2, \ldots, r-1\} \). This can be done recursively as follows. We clearly have

\[
c_{r-1,r-1}(x_0, x_1, \ldots, x_{r-2}) = 1
\]
\[
s_{r-1,r-1}(x_0, x_1, \ldots, x_{r-2}) = 0
\]

for all \( x_0, \ldots, x_{r-2} \in \{-1,1\} \). Suppose \( c_{u,r-1}(b_0, \ldots, b_{r-2}) \) and \( s_{u,r-1}(b_0, \ldots, b_{r-2}) \) have been already computed for \( u \in \{1, 2, \ldots, r-1\} \). Then, using

\[
cos(y + z) = \cosh(y) \cosh(z) + \sinh(y) \sinh(z)
\]
\[
sinh(y + z) = \cosh(y) \sinh(z) + \sinh(y) \cosh(z)
\]

and the fact that \( \cosh \) is an even function and \( \sinh \) is an odd function, we have for \( u \in \{1, 2, \ldots, r-1\} \),

\[
c_{u,r}(b_0, \ldots, b_{r-1}) = \alpha c_{u,r-1}(b_0, \ldots, b_{r-2}) + \beta b_{r-u-1} b_{r-1} s_{u,r-1}(b_0, \ldots, b_{r-2})
\]
\[
s_{u,r}(b_0, \ldots, b_{r-1}) = \alpha s_{u,r-1}(b_0, \ldots, b_{r-2}) + \beta b_{r-u-1} b_{r-1} c_{u,r-1}(b_0, \ldots, b_{r-2}),
\]

where \( \alpha = \cosh \theta \) and \( \beta = \sinh \theta \). Hence, except for determining \( \alpha \) and \( \beta \), no values of \( \cosh \) or \( \sinh \) have to be computed, and Construction 3 can be implemented with \( O(n^2) \) additions and \( O(n^2) \) multiplications.

4. A Conjecture

For the binary sequence \( B_n \) of length \( n \) obtained under Construction 3, we have computed \( M(B_n) \) for \( n \in \{1000, 2000, \ldots, 10^6\} \). The data suggest that \( M(B_n) \) is much smaller than the upper bound given in Theorem 4. Figure 1 compares \( M(B_n) \) with the function \( \sqrt{n \log \log n} \) and lends evidence to the following conjecture.

**Conjecture 5.** Let \( B_n \) be the binary sequence of length \( n \) obtained under Construction 3. Then there exist positive constants \( c_1 \) and \( c_2 \) such that, for all \( n > 1 \),

\[
c_1 \sqrt{n \log \log n} \leq M(B_n) \leq c_2 \sqrt{n \log \log n}.
\]

Some examples for small \( n \) reveal that, if \( c_2 \) in Conjecture 5 exists, then \( c_2 \) must be strictly greater than 1. It is however conceivable that

\[
\limsup_{n \to \infty} \frac{M(B_n)}{\sqrt{n \log \log n}} \leq 1.
\]

The correctness of Conjecture 5 implies that the sequences \( B_n \) are exceptional in the sense that their peak sidelobe level grows strictly more slowly than that of most binary sequences, as given in Theorem 1. Although we cannot prove Conjecture 5, in the light of Figure 1, we believe that Construction 3 meets the challenge of finding binary sequences of arbitrary lengths with small peak sidelobe level.
Figure 1. The peak sidelobe level of $B_n$ compared to $\sqrt{n \log \log n}$.

References


