BARKER SEQUENCES OF ODD LENGTH

KAI-UWE SCHMIDT AND JÜRGEN WILLMS

Abstract. A Barker sequence is a binary sequence for which all nontrivial aperiodic autocorrelations are at most 1 in magnitude. An old conjecture due to Turyn asserts that there is no Barker sequence of length greater than 13. In 1961, Turyn and Storer gave an elementary, though somewhat complicated, proof that this conjecture holds for odd lengths. We give a new and simpler proof of this result.

1. Introduction

Consider a binary sequence A of length $n > 1$, namely an element of $\{-1, 1\}^n$. We write $A(k)$ for the k-th entry in A. Define the *aperiodic autocorrelation* at shift u (where $0 \le u < n$) of A to be

$$C(u) = \sum_{k=1}^{n-u} A(k)A(k+u).$$

Notice that $C(0) = n$. All other values $C(u)$ are called the *nontrivial* aperiodic autocorrelations. There is sustained interest in binary sequences for which all of the nontrivial aperiodic autocorrelations are small (see [3] for a good survey). It is known [5] that, for each $n > 1$, there exists a binary sequence of length n such that all nontrivial aperiodic autocorrelations are at most $\sqrt{2n\log(2n)}$ in magnitude.

On the other hand, it is not known whether there exist infinitely many Barker sequences, namely binary sequences with the ideal property that the nontrivial aperiodic autocorrelations are at most 1 in magnitude. Notice that for fixed $a, b \in \{0, 1\}$, the transformation $A(k) \mapsto A(k)(-1)^{a+bk}$ preserves the Barker property. We can therefore assume without loss of generality that a Barker sequence A satisfies $A(1) = A(2) = 1$. The only known Barker sequences with this property are (writing $+$ for 1 and $-$ for -1)

$$\begin{aligned} A_3 &= [++-], & A_2 &= [++], \\ A_5 &= [+++-+], & A_4 &= [+++-], \\ A_7 &= [+++--+-], & A_4' &= [++-+], \\ A_{11} &= [+++---+---+-], \\ A_{13} &= [+++++--++-+-+]. \end{aligned}$$

Date: 23 January 2015 (revised 03 June 2015).

2010 *Mathematics Subject Classification.* 11B83, 05B10, 94A55.

K.-U. Schmidt is supported by German Research Foundation (DFG).

Indeed, it has been conjectured since at least 1960 [6] that there is no Barker sequence of length greater than 13. This conjecture is known to be true for sequences of odd length, as proven by Turyn and Storer [7].

Theorem 1 (Turyn and Storer [7])**.** *If there exists a Barker sequence of odd length n, then $n \in \{3, 5, 7, 11, 13\}$.*

Fairly deep methods have been devised to attack the case that the length is even, including the character-theoretic approach by Turyn [8] and the field-descent method by B. Schmidt [4], but the problem remains open. We refer to [3] for a brief survey and to [2] for the latest results on this problem.

The proof of Theorem 1 due to Turyn and Storer [7] is elementary, but involves an arduous inductive argument.[1] Borwein and Erdélyi [1] gave a proof using a different induction, but its overall structure is similar to that of Turyn and Storer [7]. In this paper, we offer a simpler proof of Theorem 1.

We briefly explain how our proof differs from the previous ones. For a putative Barker sequence A of odd length $n > 3$ assume that $A(1) = A(2) = 1$ and let $p + 1$ be the position of the first occurrence of -1 in A. It is not hard to show that $p \geq 3$. The crucial (and lengthy) step in the proofs of [7] and [1] is to establish that A has the following block structure

$$A(jp + 1) = A(jp + 2) = \cdots = A(jp + r)$$

for all j and r satisfying $1 \leq jp + r \leq n - p - 2$ and $1 \leq r \leq p$. Once this is established, it is easy to conclude that A cannot have many such blocks and must therefore be short.

In contrast, we do not establish such a block structure explicitly. We consider the *runs* of A, which are subsequences of maximal length consisting of equal entries (see [10] for connections between runs and autocorrelations). We assume that A starts with $e - 1$ runs whose lengths are divisible by p and that the length of the e-th run is not divisible by p. Let q be the sum of the lengths of the first e runs. It is not hard to show that $n \geq 2q - 3$. The key result is that, if $n > p + q + 1$, then

$$|C(n - p - q + 1) - C(n - p - q - 1)| \geq 4,$$

which contradicts the defining property of a Barker sequence. Therefore, we have $2q - 3 \leq n \leq p + q + 1$, from which we can easily deduce Theorem 1.

We shall make use of the following results due to Turyn and Storer [7]. In order to make this note self-contained, we include their short proofs.

Lemma 2 (Turyn and Storer [7])**.** *Suppose that A is a Barker sequence of odd length n. Then the following statements hold:*

(i) $A(k)A(n - k + 1) = (-1)^{(n+1)/2+k}$ *for each k satisfying* $1 \leq k \leq n$.
(ii) $A(k)A(k + 1) = A(2k)A(2k + 1)$ *for each k satisfying* $1 \leq k \leq \frac{n-3}{2}$.

[1] We note that [9] gives counterexamples to [7, Theorem 1 (iv)]. One can show however that, in [7, Theorem 1], the statements (ii) and (iii) imply (iv) with the corrected range $k \leq t/p - 1/2$, which is consistent with [9] and sufficient for the induction in the proof.

Proof. First note that, if u is odd, then $C(u)$ is a sum of an even number of 1 or -1, so $C(u) = 0$. The next step is to observe that, for $0 < u < n$,

$$C(u) + C(n-u) = \sum_{k=1}^{n} A(k)A(k+u),$$

where the second index is reduced modulo n if necessary. Use $xy \equiv x - y + 1 \pmod 4$ for $x, y \in \{-1, 1\}$ to see that $C(u) + C(n-u)$ is congruent to n modulo 4. Therefore, since exactly one of u and $n-u$ is odd, we find that

$$C(u) \equiv \begin{cases} 0 \pmod 4 & \text{for odd } u \\ n \pmod 4 & \text{for even } u. \end{cases} \tag{1}$$

Now count the number of 1 and -1 in the sum $C(u)$ to obtain, for $0 \le u < n$,

$$\prod_{k=1}^{n-u} A(k)A(k+u) = (-1)^{(n-u-C(u))/2}.$$

Multiply two successive equations of this form and use (1) to prove (i).

To prove (ii), use (i) to obtain, for $1 \le u \le \frac{n-1}{2}$,

$$\begin{aligned} C(n-2u+1) &= \sum_{k=1}^{2u-1} A(k)A(2u-k)(-1)^{\frac{n+1}{2}+k} \\ &= A(u)^2(-1)^{\frac{n+1}{2}+u} + 2\sum_{k=1}^{u-1} A(k)A(2u-k)(-1)^{\frac{n+1}{2}+k}. \end{aligned}$$

By (1), the left-hand side equals $(-1)^{(n-1)/2}$, so that

$$-\frac{1+(-1)^u}{2} = \sum_{k=1}^{u-1} A(k)A(2u-k)(-1)^k.$$

Count the number of 1 and -1 in the sum to find that

$$\prod_{k=1}^{u-1} A(k)A(2u-k) = 1$$

or equivalently

$$\prod_{k=1}^{2u-1} A(k) = A(u).$$

Multiplying two successive equations of this form proves (ii). □

2. Proof of Theorem 1

Suppose that A is a Barker sequence of odd length $n = 2m-1$. Since $C(1)$ is a sum of an even number of 1 or -1, we have $C(1) = 0$. This implies that A has exactly m runs. Accordingly, we associate with A the unique numbers $s_0, s_1, \ldots, s_m$ satisfying

$$0 = s_0 < s_1 < \cdots < s_{m-1} < s_m = n$$

and

$$A(s_j+1) = A(s_j+2) = \cdots = A(s_{j+1}) = (-1)^j A(1) \tag{2}$$

for all $j \in \{0,1,\ldots,m-1\}$. Note that $s_1 > 1$ implies $s_m = s_{m-1}+1$ by Lemma 2 (i), so that s_1 cannot divide all of the numbers $s_1,\ldots,s_m$. Accordingly, for $s_1 > 1$, we define e to be the smallest j such that $s_1 \nmid s_j$ (recall that we can always assume without loss of generality that A satisfies $A(1) = A(2) = 1$, so that $s_1 > 1$ is not a substantial restriction).

We shall need two lemmas.

Lemma 3. *Suppose that A is a Barker sequence of odd length $n > 5$ with $s_1 > 1$. Then s_1 and s_e are odd and $n \ge 2s_e - 3$.*

Proof. From Lemma 2 (i), we find that A must end with s_1 alternating entries, which implies that $n \ge 2s_1 - 1$. Since $n > 5$, we then conclude that, if s_1 were even, then Lemma 2 (ii) would give

$$A(s_1/2)A(s_1/2+1) = A(s_1)A(s_1+1),$$

which contradicts (2). Hence s_1 is odd and so $s_1 \ge 3$.

Writing $n = 2m-1$, the inequality $n \ge 2s_e - 3$ is equivalent to $s_e \le m+1$. To prove this, suppose for a contradiction that $s_e \ge m+2$. Consider the subsequence of A containing the five central entries of A, namely

$$(A(m-2), A(m-1), A(m), A(m+1), A(m+2)). \tag{3}$$

Lemma 2 (i) implies that $A(m-1) \ne A(m+1)$ and $A(m-2) = A(m+2)$, which means that (3) has exactly three runs and the length of the middle run is at most 2. But since $s_e \ge m+2$, the middle run must be one of the first $e-1$ runs of A, which all have length at least $s_1 \ge 3$, a contradiction.

It remains to show that s_e is odd. We know that $s_e \le (n+3)/2$. Hence, if s_e were even, then since $n > 5$, we would find from Lemma 2 (ii) that

$$A(s_e/2)A(s_e/2+1) = A(s_e)A(s_e+1),$$

which again contradicts (2) since s_1 does not divide s_e. □

Our key result is the following lemma.

Lemma 4. *Suppose that A is a Barker sequence of odd length n with $s_1 > 1$. Then $n \le s_1 + s_e + 1$.*

Proof. Since $e > 1$ and $s_1 > 1$, the lemma holds for $n \le 5$, so assume that $n > 5$. From Lemma 3 we know that s_1 and s_e are odd. Write $v = s_1 + s_e$, so that v is even, and suppose for a contradiction that $n \ge v+3$.

In what follows, we make repeated use of (2) without explicit reference. Without loss of generality, we can assume that $A(1) = 1$. Let u be an even integer satisfying $s_e + 1 \le u \le n-1$. From Lemma 2 (i) we find that

$$C(n-u+1) = \sum_{k=1}^{u-1} A(k)A(u-k)(-1)^{\frac{n+1}{2}+k},$$

which we can rewrite as

$$(-1)^{\frac{n+1}{2}} C(n-u+1) = \sum_{j=0}^{e-1}(-1)^j \sum_{k=s_j+1}^{s_{j+1}} A(u-k)(-1)^k + \sum_{k=s_e+1}^{u-1} A(k)A(u-k)(-1)^k.$$

Since $s_e + 2 \leq v \leq n-3$ by assumption, we can apply this identity with $u = v$ and $u = v+2$ to obtain

$$(4)\quad (-1)^{\frac{n+1}{2}}(C(n-v+1)-C(n-v-1)) = \sum_{j=0}^{e-1}(-1)^j S_j + R - A(v) + A(v+1),$$

where

$$S_j = \sum_{k=s_j+1}^{s_{j+1}} (-1)^k (A(v-k) - A(v-k+2))$$

for $0 \leq j \leq e-1$ and

$$R = \sum_{k=s_e+1}^{v-1} (-1)^k A(k)(A(v-k) - A(v-k+2)).$$

Since $v \geq s_e + 2$, the sum R is nonempty. However only the first summand in R is nonzero. Hence, since s_e is odd,

$$R = A(s_e+1)(A(s_1-1) - A(s_1+1)) = 2(-1)^e.$$

The sum S_j is telescoping, so we can rewrite S_j as

$$S_j = (-1)^{s_{j+1}}(A(v-s_{j+1}) - A(v-s_{j+1}+1)) - (-1)^{s_j}(A(v-s_j) - A(v-s_j+1)),$$

from which we find that

$$S_j = 0 \quad \text{for } 1 < j < e-1$$

since, by definition, $v-s_j$ and $v-s_{j+1}$ are not divisible by s_1 for $1 < j < e-1$. Moreover, we obtain

$$S_0 = 2(-1)^e - A(v) + A(v+1)$$

and

$$S_1 = -2(-1)^e \text{ and } S_{e-1} = -2 \text{ for } e > 2.$$

For $e = 2$, we have $S_1 = -4$. Substitute everything into (4) to give

$$(-1)^{\frac{n+1}{2}}(C(n-v+1) - C(n-v-1)) = 8(-1)^e - 2A(v) + 2A(v+1),$$

which contradicts the Barker property of A. Therefore $n \leq v+1$. □

We now complete our proof of the theorem. We know that A_3 and A_5 are Barker sequences of length 3 and 5, respectively, so assume that $n > 5$. As mentioned earlier, we can assume without loss of generality that $A(1) = A(2) = 1$, so that $s_1 > 1$. From Lemmas 3 and 4 we then find that

$$(5)\qquad 2s_e - 3 \leq n \leq s_1 + s_e + 1,$$

which implies $s_e \le s_1 + 4$. From Lemma 3 we know that s_1 and s_e are odd and that $s_1 \ge 3$. Since $s_1 \ge 3$, we have $e \in \{2, 3\}$ and, since $s_e - s_1$ is even, there are only the following three cases to consider.

Case 1: $e = 3$. This case forces $(s_1, s_2, s_3) = (3, 6, 7)$, so $n = 11$ by (5) and the corresponding sequence is A_{11}.

Case 2: $e = 2$ *and* $s_2 = s_1 + 2$. Here (5) implies that n equals either $2s_1 + 1$ or $2s_1 + 3$. Hence, we find from Lemma 2 (ii) that

$$1 = A(s_1 - 1)A(s_1) = A(2s_1 - 2)A(2s_1 - 1).$$

If $n = 2s_1+1$, then $A(n-2) = A(n-3)$, which forces $s_1 = 3$ by Lemma 2 (i). Therefore, in this case we have $n = 7$ and $(s_1, s_2) = (3, 5)$ and the corresponding sequence is A_7. If $n = 2s_1 + 3$, then $A(n - 4) = A(n - 5)$, which implies that $s_1 = 3$ or 5. In the first case we obtain $n = 9$ and $(s_1, s_2) = (3, 5)$. But then Lemma 2 (i) and (ii) imply $A(6) = A(7) = 1$ and $A(6)A(7) = -1$, respectively, a contradiction. In the second case we obtain $n = 13$ and $(s_1, s_2) = (5, 7)$ and the corresponding sequence is A_{13}.

Case 3: $e = 2$ *and* $s_2 = s_1 + 4$. In this case we have $n = 2s_1 + 5$ by (5). Since, by Lemma 2 (i), A must end with a block of s_1 alternating elements preceded by a block of four alternating elements, we have $n \ge 2s_2 - 1$. Hence $n \ge 2s_1 + 7$, a contradiction.

References

[1] P. Borwein and T. Erdélyi. A note on Barker polynomials. *Int. J. Number Theory*, 9(3):759–767, 2013.

[2] P. Borwein and M. J. Mossinghoff. Wieferich pairs and Barker sequences, II. *LMS J. Comput. Math.*, 17(1):24–32, 2014.

[3] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, 461:153–178, 2008.

[4] B. Schmidt. Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, 12(4):929–952, 1999.

[5] K.-U. Schmidt. Binary sequences with small peak sidelobe level. *IEEE Trans. Inform. Theory*, 58(4):2512–2515, 2012.

[6] R. Turyn. Optimum codes study. Technical report, Sylvania Electronic Systems, January 1960. Final report, Contract AF19(604)-5473.

[7] R. Turyn and J. Storer. On binary sequences. *Proc. Amer. Math. Soc.*, 12(3):394–399, 1961.

[8] R. J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15(1):319–346, 1965.

[9] J. Willms. Counterexamples to Theorem 1 of Turyn's and Storer's paper "On binary sequences". arXiv:1404.4833v2 [math.NT].

[10] J. Willms. Autocorrelations of binary sequences and run structure. *IEEE Trans. Inform. Theory*, 59(8):4985–4993, 2013.

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

E-mail address, K.-U. Schmidt: kaiuwe.schmidt@ovgu.de

Institut für Computer Science, Vision and Computational Intelligence, Fachhochschule Südwestfalen, 59872 Meschede, Germany

E-mail address, J. Willms: willms.juergen@fh-swf.de