Irreducible polynomials and Barker sequences

Peter Borwein*
Department of Mathematics and Statistics
Simon Fraser University
Burnaby, B.C. V5A 1S6 Canada
pborwein@cecm.sfu.ca

Erich Kaltofen
Department of Mathematics, Box 8205
North Carolina State University
Raleigh, North Carolina 27695-8205 USA
kaltofen@math.ncsu.edu

Michael J. Mossinghoff
Department of Mathematics, Box 6996
Davidson College
Davidson, North Carolina 28035-6996 USA
mimossinghoff@davidson.edu

Abstract

A *Barker sequence* is a finite sequence $a_0, \ldots, a_{n-1}$, each term ± 1, for which every sum $\sum_i a_i a_{i+k}$ with $0 < k < n$ is either 0, 1, or -1. It is widely conjectured that no Barker sequences of length $n > 13$ exist, and this conjecture has been verified for the case when n is odd. We show that in this case the problem can in fact be reduced to a question of irreducibility for a certain family of univariate polynomials: No Barker sequence of length $2m+1$ exists if a particular integer polynomial of degree $4m$ is irreducible over $\mathbb{Q}$. A proof of irreducibility for this family would thus provide a short, alternative proof that long Barker sequences of odd length do not exist. However, we also prove that the polynomials in question are always reducible modulo p, for every prime p.

1 Introduction

For a positive integer m, let $g_m(x)$ denote the polynomial

$$g_m(x) = x^{4m} + x^{4m-2} + \cdots + x^{2m+2} + (-1)^m(2m+1)x^{2m} + x^{2m-2} + \cdots + x^2 + 1.$$

Five of the first six of these polynomials factor over the rationals in a nice way—as a product of two irreducible polynomials, each with ± 1 coefficients:

$$\begin{aligned}
g_1(x) &= x^4 - 3x^2 + 1 = (x^2 - x - 1)(x^2 + x - 1),\\
g_2(x) &= x^8 + x^6 + 5x^4 + x^2 + 1 = (x^4 - x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 - x + 1),\\
g_3(x) &= x^{12} + x^{10} + x^8 - 7x^6 + x^4 + x^2 + 1\\
&= (x^6 - x^5 + x^4 + x^3 - x^2 - x - 1)(x^6 + x^5 + x^4 - x^3 - x^2 + x - 1),\\
g_5(x) &= x^{20} + x^{18} + x^{16} + x^{14} + x^{12} - 11x^{10} + x^8 + x^6 + x^4 + x^2 + 1\\
&= (x^{10} - x^9 + x^8 + x^7 - x^6 + x^5 + x^4 + x^3 - x^2 - x - 1)\\
&\quad \cdot (x^{10} + x^9 + x^8 - x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + x - 1),\\
g_6(x) &= x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} + 13x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1\\
&= (x^{12} - x^{11} + x^{10} - x^9 + x^8 + x^7 - x^6 - x^5 + x^4 + x^3 + x^2 + x + 1)\\
&\quad \cdot (x^{12} + x^{11} + x^{10} + x^9 + x^8 - x^7 - x^6 + x^5 + x^4 - x^3 + x^2 - x + 1).
\end{aligned}$$

One might expect some similar factorizations to appear for larger m, but, curiously, no other polynomials $g_m(x)$ are even known to be reducible! In fact, the polynomials shown here are the only reducible ones in the sequence up to

[*] Research supported in part by NSERC of Canada and MITACS

$m = 1000$. In this note, we show how the question of irreducibility for these polynomials is connected to an old and difficult problem in combinatorial optimization involving certain binary sequences with remarkable properties, known as *Barker sequences*. We show that establishing that $g_m(x)$ is irreducible for all $m \geq 7$ would provide a simple proof that Barker sequences of odd length do not exist. However, we also demonstrate that the polynomials $g_m(x)$ are reducible mod p, for *every* prime p. Consequently, many standard tests for irreducibility do not directly apply for these polynomials.

2 Barker Sequences

We begin by recalling the definition of a Barker sequence, and describing some of its properties. For a sequence of integers a_0, a_1, $\ldots$, a_{n-1}, each one ± 1, and for an integer k with $|k| < n$, define the *kth aperiodic autocorrelation* of the sequence by

$$c_k = \sum_{i=0}^{n-1-k} a_i a_{i+k} \tag{1}$$

if $k \geq 0$, and similarly set $c_{-k} = \sum_{i=k}^{n-1} a_i a_{i-k} = c_k$. The value of c_0 is therefore n, independent of the choice of signs in the a_k. This number is called the *peak autocorrelation*. The other c_k are the *off-peak autocorrelations*, and sequences with especially small off-peak autocorrelations are of great interest in applications in communications. By considering the parity of the number of terms in the sum (1), we see that the best we can possibly achieve is $|c_k| \leq 1$ for each nonzero k, so in fact $c_k = \pm 1$ if $n - k$ is odd and $c_k = 0$ otherwise. In his 1953 paper [1], Barker asked if there exist sequences $\{a_k\}$ in which each off-peak autocorrelation c_k is 0 or -1, and sequences achieving the more symmetric condition $|c_k| \leq 1$ for $k \neq 0$ are known today as *Barker sequences.*

Since negating the terms of a sequence $\{a_k\}$ does not disturb its autocorrelations, and negating every other term does not affect the magnitudes of its autocorrelations, we may assume that $a_0 = a_1 = 1$. With this normalization, there are just eight known Barker sequences. These are displayed in Table 1, where we use + and - to represent $+1$ and -1, respectively. Only three of these satisfy the more strict condition requested by Barker—the ones of length 3, 7, and 11.

n	Barker sequence
2	++
3	++-
4	+++-
4	++-+
5	+++-+
7	+++--+-
11	+++---+--+-
13	+++++--++-+-+

Table 1: Barker sequences with $a_0 = a_1 = 1$.

It is widely conjectured that this list forms the complete set of Barker sequences, but this problem remains open and seems surprisingly hard. Before describing how this problem is related to the polynomials $g_m(x)$, we first record some properties of Barker sequences. The following results were established by Turyn and Storer [7,8]; we include the proof here for the reader's convenience.

Theorem 1. *Suppose a_0, a_1, $\ldots$, a_{n-1} is a sequence of integers with each $a_i = \pm 1$, and let $\{c_k\}$ denote the sequence of its aperiodic autocorrelations. Then*

$$c_k + c_{n-k} \equiv n \mod 4.$$

Suppose further that the sequence $\{a_k\}$ is a Barker sequence. If n is odd, then

$$a_k a_{n-1-k} = (-1)^{\frac{n-1}{2}+k} \tag{2}$$

for $0 \leq k < n$, and $c_k + c_{n-k} = (-1)^{(n-1)/2}$ for $0 < k < n$. If n is even and $n > 2$, then $n = 4m^2$ for some integer m, and $c_{n-k} = -c_k$ for $0 < k < n$.

Proof. Since c_k records the difference between the number of positive and negative terms in $\sum_{i=0}^{n-1-k} a_i a_{i+k}$, it follows that

$$\prod_{i=0}^{n-k-1} a_i a_{i+k} = (-1)^{(n-k-c_k)/2} \tag{3}$$

for $0 \leq k < n$. Multiplying this product by the same expression with k replaced by $n-k$, we obtain

$$(-1)^{(n-c_k-c_{n-k})/2} = \prod_{i=0}^{k-1} a_i a_{i+n-k} \prod_{i=0}^{n-k-1} a_i a_{i+k} = 1,$$

so $c_k + c_{n-k} \equiv n \bmod 4$. On the other hand, multiplying (3) by the same equation where k is replaced by $k+1$ (and taking $c_n = 0$), we compute that

$$a_k a_{n-1-k} = (-1)^{n-k-\frac{1}{2}(1+c_k+c_{k+1})} \tag{4}$$

for $0 \leq k < n$. Assume now that $\{a_k\}$ forms a Barker sequence of length n, so the off-peak autocorrelation c_k is 0 if n and k have the same parity, and ± 1 otherwise. If n is odd and $0 < k < n$, then exactly one of c_k and c_{n-k} is 0, and since $c_k + c_{n-k} \equiv n \bmod 4$, it follows that $c_k = (-1)^{(n-1)/2}$ when k is even. Therefore, $c_k + c_{n-k} = (-1)^{(n-1)/2}$ for $0 < k < n$. Further, we see that $c_k + c_{k+1} = (-1)^{(n-1)/2}$ for $0 < k < n$, and combining this with (4) establishes (2).

If n is even, then $c_k = 0$ for even $k \neq 0$, so in particular $c_2 + c_{n-2} = 0$ when $n > 2$, and therefore $n \equiv 0 \bmod 4$ in this case. It follows then that $c_k + c_{n-k} = 0$ when $n \geq 4$ and $0 < k < n$. Last, since

$$\left(\sum_{i=0}^{n-1} a_i\right)^2 = c_0 + \sum_{k=1}^{n-1}(c_k + c_{n-k}) = n,$$

we see that n is a perfect square in this case. □

Many additional restrictions on Barker sequences are known. Turyn and Storer [7] proved that if the length n of a Barker sequence is odd, then $n \leq 13$, so the complete list for this case appears in Table 1. It follows from this that no additional sequences satisfy Barker's original requirement for sequences whose off-peak autocorrelations are all 0 or -1, since Theorem 1 implies that any such sequence must have length $n \equiv 3 \bmod 4$. For the case when the length is even, several additional restrictions are known on m if $n = 4m^2$: m must be odd and cannot be a prime power [2, sec. 2D and 4C; 5, 9], every prime divisor p of m must satisfy $p \equiv 1 \bmod 4$ [4], and if $m > 1$ then in fact $m > 5 \cdot 10^{10}$ [6]. Thus, any additional Barker sequences must have length exceeding 10^{22}! More information on Barker sequences, and their connection to other open problems in analysis and number theory, appears in [3].

3 A Question of Irreducibility

The proof of Turyn and Storer that no Barker sequences of odd length n exist for $n > 13$ is elementary, though somewhat complicated, and relies on showing that long Barker sequences of odd length must exhibit certain patterns. We describe here a possible alternative route to proving this result, in the hope of spurring further research.

Theorem 2. *If the polynomial*

$$g_m(x) = (-1)^m(2m+1)x^{2m} + \sum_{k=1}^{m}\left(x^{2m+2k} + x^{2m-2k}\right)$$

is irreducible over $\mathbb{Q}$, then no Barker sequence of length $2m+1$ exists.

We require a brief definition before supplying the proof. For a polynomial $f(x)$ with $f(0) \neq 0$, we define its *reciprocal polynomial* $f^*(x)$ by $f^*(x) := x^{\deg f} f(1/x)$. Also, for $f(x) \in \mathbb{Z}[x]$ with $f(0) \neq 0$, we say that f is *self-reciprocal* if $f = \pm f^*$.

Proof of Theorem 2. Suppose $\{a_k\}$ is a Barker sequence of length $2m+1$, and let $f_m(x) = \sum_{k=0}^{2m} a_k x^k$. By Theorem 1, the aperiodic autocorrelation c_k is 0 if k is odd and $(-1)^m$ if $k \neq 0$ and k is even. Thus

$$\begin{aligned} f_m(x) f_m^*(x) &= \sum_{k=-m}^{m} c_{2k} x^{2k+2m} \\ &= (2m+1)x^{2m} + \sum_{k=1}^{m} (-1)^m \left(x^{2m+2k} + x^{2m-2k}\right), \end{aligned}$$

and so $g_m(x) = (-1)^m f_m(x) f_m^*(x)$. □

We conjecture that the polynomial $g_m(x)$ is in fact irreducible for every $m > 6$. However, we find that these polynomials are reducible mod p, for every prime number p. This follows immediately from the following more general statement.

Theorem 3. *Suppose $f(x)$ is an even, self-reciprocal polynomial with integer coefficients and* $\deg(f) \geq 4$. *Then $f(x)$ is reducible mod p for every prime p.*

Proof. If $f = -f^*$ then $f(\pm 1) = 0$ so f is reducible over $\mathbb{Q}$. If $f = f^*$ and $\deg(f) = 4n+2$ then $f(\pm i) = 0$, so again f is reducible over $\mathbb{Q}$ for $n \geq 1$. Suppose then that $f = f^*$ and $\deg(f) = 4n$ with $n \geq 1$, and write $f(x) = g(x^2)$. Clearly $f(x) \equiv g(x)^2 \bmod 2$, so suppose p is an odd prime, and $g(x)$ is irreducible mod p. Let α be a root of g in its splitting field $\mathbb{F}_{p^{2n}}$ over $\mathbb{F}_p$, so that

$$g(x) = \prod_{k=0}^{2n-1} \left(x - \alpha^{p^k}\right).$$

Let γ be a primitive element of $\mathbb{F}_{p^{2n}}$, and let $\alpha = \gamma^t$ for some integer t. Since g is self-reciprocal, α^{-1} is also a root of g, so $\alpha^{-1} = \gamma^{-t} = \alpha^{p^j} = \gamma^{tp^j}$ for some positive integer $j < 2n$. Then $\gamma^{tp^{2j}} = \gamma^{-tp^j} = \gamma^t$, so $\alpha^{p^{2j}-1} = 1$, and consequently $j = n$. Therefore $\gamma^{t(p^n+1)} = 1$, so $(p^n - 1) \mid t$ and thus t is even. Let $\beta = \gamma^{t/2}$. Then

$$f(x) = \prod_{k=0}^{2n-1} \left(x + \beta^{p^k}\right) \cdot \prod_{k=0}^{2n-1} \left(x - \beta^{p^k}\right),$$

and each of these products lies in $\mathbb{F}_p[x]$. □

This result would appear to make the determination of the irreducibility of the polynomials $g_m(x)$ a more challenging proposition!

References

[1] R. H. Barker, *Group synchronizing of binary digital systems* (1953), 273–287.

[2] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, Berlin, 1971.

[3] P. Borwein and M. J. Mossinghoff, *Barker sequences and flat polynomials* (2008).

[4] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory Ser. A **55** (1990), 49–59.

[5] S. Eliahou and M. Kervaire, *Barker sequences and difference sets*, Enseign. Math. (2) **38** (1992), 345–382, Corrigendum, ibid. **40** (1994), no. 1–2, 109–111.

[6] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), 171–188.

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

[8] R. Turyn, *On Barker codes of even length*, IEEE Trans. Inform. Theory **51** (1963), 1256.

[9] ———, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.