WIEFERICH PAIRS AND BARKER SEQUENCES

MICHAEL J. MOSSINGHOFF

Abstract. We show that if a Barker sequence of length $n > 13$ exists, then either $n = 189\,260\,468\,001\,034\,441\,522\,766\,781\,604$, or $n > 2 \cdot 10^{30}$. This improves the lower bound on the length of a long Barker sequence by a factor of more than 10^7. We also show that all but fewer than 1600 integers $n \leq 4 \cdot 10^{26}$ can be eliminated as the order of a circulant Hadamard matrix. These results are obtained by completing extensive searches for Wieferich prime pairs (q, p), which are defined by the relation $q^{p-1} \equiv 1 \bmod p^2$, and analyzing their results in combination with a number of arithmetic restrictions on n.

1. Introduction

A *binary sequence* of length n is a sequence $a_0, a_1, \ldots, a_{n-1}$ whose terms are all ±1. For an integer k with $0 \leq k < n$, define the *kth aperiodic autocorrelation* c_k of such a sequence by

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

and define its *kth periodic autocorrelation* γ_k by

$$\gamma_k := \sum_{i=0}^{n-1} a_i a_{(i+k \bmod n)}.$$

Certainly $c_0 = \gamma_0 = n$; this is the *peak* autocorrelation. The others are known as the *off-peak* or *out-of-phase* autocorrelations.

Binary sequences whose off-peak autocorrelations are uniformly small are of considerable interest in a number of problems in combinatorics and signal processing. In the aperiodic case, the optimal situation occurs if $c_k = 0$ whenever $n - k$ is even and $c_k = \pm 1$ whenever $n - k$ is odd. A sequence achieving this condition for each $k > 0$ is known as a *Barker sequence*, since Barker [1] first noted their utility in certain problems in signal processing. (Barker in fact asked for sequences satisfying the stricter condition that $c_k \in \{0, -1\}$ for $0 < k < n$, but it is standard to allow the broader, symmetric restriction $|c_k| \leq 1$.) It is easy to verify that if $\{a_k\}$ is a Barker sequence of length n, then so are $\{-a_k\}$, $\{(-1)^k a_k\}$, and $\{a_{n-1-k}\}$. After accounting for these symmetries, only seven Barker sequences with length $n \geq 2$ are known. These are listed in Table 1. It is widely conjectured that no additional Barker sequences exist.

Turyn and Storer [30] established that the maximal length of a Barker sequence of odd length is 13, so the list in Table 1 is complete for odd n. The question of

Date: June 4, 2009.

2000 *Mathematics Subject Classification.* Primary: 11B85; Secondary: 05B10, 11A41, 94A55.

Key words and phrases. Barker sequence, circulant Hadamard matrix, Wieferich prime pair.

Research supported in part by NSA grant number H98230-08-1-0052.

Table 1. Known Barker sequences.

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

the existence of a Barker sequence of even length $n > 4$ is a longstanding unsolved problem in combinatorial optimization.

For the periodic case, binary sequences whose off-peak autocorrelations are constant correspond to cyclic difference sets. Recall that a cyclic difference set S with parameters (n, k, λ) is a k-element subset of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ which has the property that each nonzero element of $\mathbb{Z}/n\mathbb{Z}$ can be expressed in exactly λ different ways as a difference of elements of S. For a binary sequence $\{a_i\}$ of length n with constant periodic off-preak autocorrelation γ, the corresponding difference set is $S = \{i : a_i = -1\}$, and has $\lambda = k - (n - \gamma)/4$. (See for instance [7] for a proof.)

The periodic and aperiodic off-peak autocorrelations for a binary sequence of length n are certainly related by

$$\gamma_k = c_k + c_{n-k}.$$

Further, it is well-known [3, 30] that if $\{a_k\}$ is a Barker sequence of length n, then

$$c_k + c_{n-k} = \begin{cases} (-1)^{(n-1)/2}, & \text{if } n \text{ is odd,} \\ 0, & \text{if } n \geq 4 \text{ is even.} \end{cases}$$

Therefore, a Barker sequence has constant periodic off-peak autocorrelation $\gamma \in \{-1, 0, 1\}$, and gives rise to a cyclic difference set. (Not all such cyclic difference sets arise from Barker sequences, however.) In the case of interest in the Barker sequence problem, where n is even and $n \geq 4$, this question is a special case of a well-known open problem in design theory, as the case $\gamma = 0$ in the periodic formulation coincides precisely with the question of the existence of circulant Hadamard matrices.

Recall that a *Hadamard matrix* is a square matrix H whose entries are all ± 1 and whose rows are mutually orthogonal. Thus, if H is $n \times n$, then $HH^T = nI_n$, and we say H has order n. Its determinant thus achieves the upper bound in Hadamard's well-known inequality. A *circulant matrix* has the property that each row after the first is a cyclic shift to the right by one position of the prior row. For example, the matrix obtained by using the Barker sequence of length 4 from Table 1,

$$H_4 = \begin{bmatrix} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{bmatrix},$$

is a circulant Hadamard matrix. No such matrices are known with order $n > 4$. The question of their existence is a well-known open problem in design theory, dating at least to the monograph of Ryser [24, sec. 9.1].

A number of restrictions are known on permissible values of n in the circulant Hadamard matrix problem, and even stronger conditions on n have been established in the Barker sequence problem. We review these restrictions in section 2, and describe their connection with a problem in number theory involving certain pairs of prime numbers. A pair of primes (q, p) is said to be a *Wieferich prime pair* if $q^{p-1} \equiv 1 \bmod p^2$. Certainly, basic group theory ensures that $q^{p-1} \equiv 1 \bmod p$, but solutions modulo p^2 are rather rare when $q < p$. Wieferich prime pairs arise in many problems in number theory, including the study of Fermat's Last Theorem, where Wieferich [31] established in 1909 that if $x^p + y^p = z^p$ with $p \nmid xyz$ then $(2, p)$ is such a pair; others (e.g., [13]) later established the same fact for (q, p) for a number of small primes q. These pairs also arise in Mihăilescu's solution of Catalan's problem [19, 20], which asked if 8 and 9 are the only consecutive powers (indeed they are). Wieferich pairs appear as well in recent work on the question of the existence of odd perfect numbers [23], probably the oldest unsolved problem in mathematics.

In sections 3 and 4, we describe how a large search for Wieferich prime pairs allows us to increase the lower bound on the length of any additional Barker sequences by a factor of more than 10^7. In fact, we can eliminate all but one possible value of n up to $2 \cdot 10^{30}$ by analyzing our data in combination with the known restrictions on n in this problem. For the circulant Hadamard matrix problem, our method establishes that there are fewer than 1600 values for n up to $4 \cdot 10^{26}$ that cannot be eliminated as a possible order of such a matrix.

Since Wieferich prime pairs have independent interest in several problems in number theory, section 5 describes our searches for these objects, and summarizes some results of particular interest.

2. Some known restrictions

It is well-known that the order n of a Hadamard matrix must be a multiple of 4 (except for $n = 1$ and $n = 2$), and that the order of a circulant Hadamard matrix must be a square [24, sec. 9.1]. Write $n = 4m^2$. In 1965, Turyn [28] (see also [2, sec. 2D and 4C; 7]) proved that m must be odd and cannot be a prime power. Turyn also established a more complicated requirement in the same article known as the self-conjugacy test. For integers r and s, we say r is *semiprimitive* mod s if there exists an integer j such that $r^j \equiv -1 \bmod s$. We say r is *self-conjugate* mod s if each prime divisor p of r is semiprimitive mod s_p, where s_p is the largest divisor of s not divisible by p. Turyn proved the following theorem.

Theorem 1. *Suppose $n = 4m^2$ is the order of a circulant Hadamard matrix, and r and s are integers with $r \mid m$, $s \mid n$, and $\gcd(r, s)$ has $k \geq 1$ distinct prime factors. If r is self-conjugate mod s, then $rs \leq 2^{k-1}n$.*

In 1992, Jedwab and Lloyd [14] derived a number of useful special cases of this general criterion in their analysis of permissible lengths of Barker sequences. We cite one such special case here. For the proof, one merely selects $r = p^k$ and $s = 2p^{2k}$ in Theorem 1.

Corollary 2. *Suppose $p^k \mid m$, for an odd prime p and positive integer k. If $p^{3k} > 2m^2$ then no circulant Hadamard matrix of order $n = 4m^2$ exists.*

Another strong condition was obtained by Leung and Schmidt in 2005 [18], following and extending the influential work of Schmidt [25, 26]. For an integer m and prime p, let $\nu_p(m)$ denote the multiplicity of p in the prime factorization of m. Also, for a prime q, let m_q denote the q-free and squarefree part of m, so

$$m_q = \prod_{\substack{p \mid m \\ p \neq q}} p.$$

Next, let $b(p, m)$ denote the integer

$$b(p, m) := \max_{\substack{q \mid m \\ q \neq p}} \left\{ \nu_p(q^{p-1} - 1) + \nu_p(\operatorname{ord}_{m_q}(q)) \right\}. \tag{1}$$

Here, q ranges over the prime divisors of m, and $\operatorname{ord}_u(x)$ denotes the multiplicative order of x in the group $(\mathbb{Z}/u\mathbb{Z})^*$. Note that $b(p, m) \geq 1$ for all p, assuming m is not a power of p, since $q^{p-1} \equiv 1 \bmod p$ for any $q \neq p$. Finally, let $F(m)$ denote the integer with the same prime factors as m, but with multiplicities determined by the values of the $b(p, m)$:

$$F(m) := \gcd\left(m^2, \prod_{p \mid m} p^{b(p,m)}\right). \tag{2}$$

Thus, if a prime p has multiplicity k in m, then the multiplicity of p in $F(m)$ is at least 1 and at most $2k$. Leung and Schmidt proved that $F(m)$ must in fact be rather large if a circulant Hadamard matrix of order $4m^2$ exists. They established the following theorem, where $\varphi(\cdot)$ denotes Euler's totient function.

Theorem 3. *Using the notation above, if $n = 4m^2$ is the order of a circulant Hadamard matrix, then $F(m) \geq m\varphi(m)$.*

Naturally, the same restrictions hold for Barker sequences. However, an additional important restriction was established in this problem by Eliahou, Kervaire, and Saffari in 1990 [8].

Theorem 4. *If $n = 4m^2$ is the length of a Barker sequence, and p is a prime number with $p \mid m$, then $p \equiv 1$ mod 4.*

We remark that some proscriptions on particular symmetries are also known in these problems. In 1965, Brualdi [5] showed that a circulant Hadamard matrix cannot be symmetric, and in 1989, Fredman, Saffari, and Smith [11] proved that a Barker sequence may not be palindromic. Since we are interested only in allowable values for n, these restrictions are not exploited in the present study. We also remark that a number of connections between the question of the existence of Barker sequences and some analytic and algebraic problems on polynomials with restricted coefficients are described in [3, 4].

These results have been used to disqualify a number of integers as possible orders of circulant Hadamard matrices, or lengths of Barker sequences. In 1968, Turyn [29] used Theorem 1 to show that if $n = 4m^2$ and $m > 1$ in either problem, then $m \geq 55$ (so $n \geq 12\,100$). In 1999, Schmidt [25] employed an earlier version of Theorem 3, combined with Theorem 4, to show that $m \geq 165$ in the circulant Hadamard matrix problem, so $n \geq 108\,900$. Leung and Schmidt [18] improved this in 2005 to $m \geq 11\,715 = 3 \cdot 5 \cdot 11 \cdot 71$. For the Barker sequence problem, in 1992 both Eliahou and Kervaire [7] and Jedwab and Lloyd [14] showed that $m \geq 689$ (so $n \geq 1\,898\,884$), and the latter paper also noted just six permissible values of m below 5000. Schmidt [25] established that $m > 10^6$ in 1999, and Leung and Schmidt [18] proved that $m > 5 \cdot 10^{10}$, so $n > 10^{22}$, without employing the self-conjugacy conditions of Theorem 1 or Corollary 2.

We next describe a large computational investigation, centering on the conditions of Theorem 3, but employing all of these restrictions, with the goal of eliminating as many values of n from contention as possible as the length of a Barker sequence, or the order of a circulant Hadamard matrix.

3. Algorithms

Before describing our method for searching for permissible values of n in these problems, we first note two helpful simplifications. First, we may assume that $F(m) = m^2$ in the Barker sequence problem, which is the maximum possible value for $F(m)$. To see this, suppose that $b(p, m) \leq 2\nu_p(m) - 1$, for some prime $p \mid m$. Then $F(m) \leq m^2/p$. If $F(m) \geq m\varphi(m) = m^2 \prod_{q|m}(1 - 1/q)$, then it follows that

$$\prod_{q|m} \left(1 - \frac{1}{q}\right)^{-1} \geq p \geq 5,$$

since $p \equiv 1 \bmod 4$. However, the product on the left side grows so slowly that its value never exceeds 1.7 for any possible value of $m \leq 10^{15}$, and we consider no larger m in this study. In the circulant Hadamard matrix problem, the product over all odd primes could conceivably exceed 3, but not 4, in the range we study, so we may assume that $F(m) = m^2$ if $3 \nmid m$ and $F(m) = m^2$ or $m^2/3$ otherwise.

Second, we may assume that m is squarefee. It is clear that the value of $b(p, m)$ given by (1) depends only on the squarefree part of m. We may therefore search only for squarefree m that satisfy Theorem 3, then test if any non-squarefree multiples of m are also permissible by observing the values of the $b(p, m)$.

We describe an algorithm then for computing all squarefree integers m with $F(m) = m^2$ and $m \leq M$, where M is some fixed bound. In view of (1) and (2), we must find all integers $m \leq M$ with the property that for each prime divisor p of m, there exists another prime divisor q of m such that

$$q^{p-1} \equiv 1 \bmod p^2 \tag{3}$$

or

$$p \mid \operatorname{ord}_{m/q}(q). \tag{4}$$

In the former case, the primes (q, p) form a Wieferich pair. For the latter case, a necessary condition is certainly that $p \mid \varphi(m/q)$, so we require that $p \mid (r - 1)$ for some prime $r \mid m$ with $r \neq q$. Thus, we may search for qualifying integers $m \leq M$ by constructing a large directed graph $D = D(M)$. Its vertices are (a subset of) the primes up to M, and there are two types of edges. We place a *solid edge* $q \to p$ if condition (3) holds, that is, if (q, p) is a Wieferich prime pair. We place a *flimsy edge* $r \rightsquigarrow p$ if $p \mid (r - 1)$. Thus, a solid edge $q \to p$ indicates that $b(p, m) \geq 2$ if $pq \mid m$; a flimsy edge $r \rightsquigarrow p$ means that it is possible that $b(p, m) \geq 2$ if $pr \mid m$ and m has at least one additional prime divisor. In fact, one can be reasonably confident that $b(p, m) \geq 2$ in this case, since all but at most $1/p$ of the elements in the underlying abelian group have order divisible by p. Thus, if p is sizable, or if m has several prime factors, then this is nearly certain.

In the Barker sequence problem, we modify our construction of D by including only primes congruent to 1 mod 4. In the circulant Hadamard matrix problem, we include all odd primes, but allow for the possibility that $F(m) = m^2/3$ simply by inserting a flimsy edge $q \rightsquigarrow 3$ for each prime q in the graph. Thus, in these two problems, a candidate value for m corresponds to an induced subgraph of D, each of whose vertices has positive indegree. In particular, such a subgraph must contain a cycle. We therefore require two algorithms for constructing the candidate values of m: a cycle enumerator, and a method for augmenting the cycles we find with additional outgoing edges. Our restriction that $m \leq M$ implies that we may also impose a restriction on the length of the cycles we seek, and allows us to trim the search in the augmentation routine as well.

We describe our algorithm for constructing values for m that satisfy Theorem 3 (and Theorem 4 for the Barker sequence problem) by describing its four principal components: graph construction, cycle enumeration, cycle augmentation, and some final processing.

3.1. **Graph construction.** We begin by searching for Wieferich prime pairs (q, p) with $q < p$, where bounds on p and q are determined in a particular way by our choice of M. Specific bounds in each problem are shown in section 4. This is a large, distributed computation, requiring the vast majority of the CPU time used in this project. The pairs we discover determine an initial vertex set V_0 for our graph D. Next, for each prime $q \in V_0$, we search for Wieferich prime pairs (q, p) with $p < \min\{q, M'\}$, where $M' \geq \sqrt{M}$ is another parameter of the algorithm. These pairs may introduce additional primes not in V_0, so we search for additional pairs (q, p) with $p < \min\{q, M'\}$ for each such new prime q, and continue this process until no new primes are discovered. Let V_1 denote the entire set of primes appearing in the Wieferich pairs found through this stage. After this, for each prime $q \in V_1$, we find all primes $r \mid (q - 1)$ and add the corresponding links $q \rightsquigarrow r$ to the graph. We iterate this process on any new primes that appear in this way, until forming a stable set of primes V_2. If $V_2 \neq V_1$, we perform the descending Wieferich pair search on $V_2 \setminus V_1$, and on new primes that appear after this to form V_3, then determine all flimsy links from the primes in $V_3 \setminus V_2$ to create V_4, and so on. We continue this process until $V_k = V_{k-1}$. This completes the construction of the directed graph D.

3.2. **Cycle enumeration.** The directed graph D is represented by using adjacency lists. The vertices of the graph are stored in a balanced binary search tree, and each node of the tree contains two lists of nodes adjacent to the current node: one for solid links; the other for flimsy links. Each element of each of these lists is the address of the corresponding node in the tree. In this way, any node in the tree can be found quite rapidly given the prime number it stores by using the tree structure, and the edges of the graph can be traversed very easily by using the adjacency lists.

We implement Tarjan's algorithm [27] for enumerating all cycles in a directed graph, amending it slightly to accept an option for returning only cycles with length bounded by a parameter ℓ. This option is needed for analyzing the graph constructed for the circulant Hadamard matrix problem, which otherwise produces an overwhelming number of cycles.

3.3. **Cycle augmentation.** Given a cycle C in D, this algorithm determines connected subgraphs G of D containing C with the property that the product of the vertices in G is at most M. We implement the following recursive algorithm to produce all such graphs.

Input. A directed graph D containing a cycle C, and a positive integer M.

Output. All induced subgraphs G of D containing C having vertex product at most M, with the property that each vertex of G can be reached from a vertex in C using only edges in G.

Description.

Step 0. Print C. Mark each vertex of C as visited, and admit each of these to the set S_0. Perform Step 1 using $G = C$, $m =$ the product of the vertices of C, and $z = \lfloor M/m \rfloor$.

Step 1. Given G, m, and z. Perform Step 2 for each vertex v of G.

Step 2. Suppose $v \in S_k$. For each vertex w in either adjacency list of v, perform Step 3.

Step 3. If w has not been visited, $w \leq z$, and $w > \max(S_{k+1})$, then perform Step 4.

Step 4. Mark w as visited and admit w to S_{k+1}. Let G' denote the graph obtained by adding the link from v to w to G. Print G'. Invoke Step 1 on G', using mw and $\lfloor z/w \rfloor$ in place of m and z. Then remove w from S_{k+1} and mark w as unvisited.

Maintaining the sets S_k in the algorithm greatly reduces redundancy in the output. Both this method and the cycle detection algorithm were implemented in C++.

3.4. **Final processing.** Since each flimsy link $p \rightsquigarrow r$ in our graph D carries an element of uncertainty, we must check that each subgraph G produced by the cycle augmenter indeed corresponds to a viable integer candidate m. This check, performed in Maple, simply computes the value of $b(p,m)$ for each prime $p \mid m$ and checks if $F(m) \geq m\varphi(m)$. At the same time, it determines if any non-squarefree multiples of m have this property by checking these $b(p,m)$ values. In this way, we determine all integers up to M that pass the criteria of Theorem 3 (and Theorem 4 for the Barker sequence problem).

4. Results

We describe the parameters employed in our algorithms, and the results obtained from them, first for the Barker sequence problem, and then for the circulant Hadamard matrix problem.

4.1. **Barker sequences.** We first take $M = 10^{14}$, and begin by searching for Wieferich prime pairs (q,p) with $q < p$ and both primes congruent to 1 mod 4. This search was performed in several phases, so that small primes q were checked against many more primes p than larger q. The bounds on p and q used in each phase are shown in Table 2, together with the number of such pairs found in each case, and the total CPU time, in gigahertz-weeks. For example, the prime $q = 5$ was tested against all $p < 10^{14}$, and primes q between 13 and 97 were checked against all $p < 10^{13}$. All of the searches for Wieferich pairs were performed at the Centre for Interdisciplinary Research in the Mathematical and Computational Sciences (IRMACS) at Simon Fraser University in British Columbia, Canada, using a number of dual-core, 2.5 GHz, PowerPC-based Apple workstations.

TABLE 2. Wieferich pair searches, $p \equiv q \equiv 1 \bmod 4$, $q < p$.

q Bound	p Range	Pairs	GHz-wks
10^8	$[0, 10^8]$	88447	81.0
10^6	$[10^8, 10^9]$	2355	9.2
10^5	$[10^9, 10^{10}]$	277	15.7
10^4	$[10^{10}, 10^{11}]$	26	22.8
10^3	$[10^{11}, 10^{12}]$	4	29.6
10^2	$[10^{12}, 10^{13}]$	0	42.1
10	$[10^{13}, 10^{14}]$	0	58.5

The 91 109 pairs found here determine our initial set V_0 of 174 575 primes for our directed graph D. The search for descending Wieferich pairs starting with this set of primes, and using $M' = 10^8$, produces 224 422 solid links (q, p) with $q > p$, and determines our set V_1 of 202 231 primes. The calculation of all primes r satisfying $r \equiv 1 \bmod 4$ and $r \mid (p-1)$, for some prime $p \in V_1$, produces 242 252 flimsy links for D, and creates V_2, with 216 359 primes. We then find $|V_3| = 216\,903$ after a subsequent search for descending Wieferich prime pairs, then $|V_4| = 216\,910$ after another prime divisor check, and then $V_5 = V_4$. In all, we collect 330 689 solid links and 242 838 flimsy links on 216 910 vertices for our graph D.

Our cycle enumerator detects 2687 different cycles in our graph, with lengths ranging from 2 to 50. (Using $M = 10^{14}$, no cycle of interest could possibly have length larger than 10, so the length restriction available in our method could be employed with $\ell = 10$.) Only five of these have the property that $m \leq M$:

$$5 \rightarrow 53\,471\,161 \rightsquigarrow 5, \tag{5}$$

$$5 \rightarrow 53\,471\,161 \rightarrow 193 \rightarrow 5, \tag{6}$$

$$5 \rightarrow 188\,748\,146\,801 \rightarrow 5, \tag{7}$$

$$41 \rightarrow 138\,200\,401 \rightsquigarrow 2953 \rightsquigarrow 41, \tag{8}$$

$$5 \rightarrow 6\,692\,367\,337 \rightarrow 1601 \rightarrow 5. \tag{9}$$

The first cycle (5) is certainly disqualified, since a flimsy link requires a third prime to be effective. Cycle (8) is also disallowed, since here we are unlucky and $b(41, m) = 1$. However, an augmentation of one of these graphs may form a permissible subgraph of D, so we use all of these as input to our cycle augmentation algorithm, using $M = 10^{14}$. After final processing on its output, we obtain a short list of five permissible values for m up to this bound.

$$51\,599\,670\,365 = 5 \cdot 193 \cdot 53\,471\,161, \tag{10}$$

$$257\,998\,351\,825 = 5^2 \cdot 193 \cdot 53\,471\,161, \tag{11}$$

$$943\,740\,734\,005 = 5 \cdot 188\,748\,146\,801, \tag{12}$$

$$53\,572\,400\,532\,685 = 5 \cdot 1601 \cdot 6\,692\,367\,337, \tag{13}$$

$$83\,661\,685\,751\,365 = 5 \cdot 41 \cdot 2953 \cdot 138\,200\,401. \tag{14}$$

We remark that the search described in [18] for m that satisfy the constraints of Theorems 3 and 4 ceased at $m = 5 \cdot 10^{10}$; the smallest qualifying value of m (10) in fact lies just beyond this bound. We add also that the short cycle (7) forms a *double Wieferich prime pair*, since both $(5, 188\,748\,146\,801)$ and $(188\,748\,146\,801, 5)$ are Wieferich prime pairs. Double Wieferich prime pairs are extremely rare; this one was in fact found by Keller and Richstein in 2005 [15]. It is the only known such pair in which both primes are congruent to 1 mod 4.

We may now ask if any of these qualifying values of m also pass the self-conjugacy restrictions of Theorem 1 and Corollary 2. The large prime test of Corollary 2 eliminates all but (14), and this last one fails Turyn's test with $r = 5 \cdot 2953$ and $s = 138200401^2 r^2$, since $5^{195768344658194100} \equiv -1 \bmod s/25$ and $2953^{2387418837295050} \equiv -1 \bmod s/2953^2$. It follows that there are no Barker sequences with length n satisfying $13 < n \leq 4 \cdot 10^{28}$.

We can extend this bound by a significant margin with a modest amount of additional computation if we employ Corollary 2. By choosing $M = 10^{15}/\sqrt{2}$, we see that Corollary 2 automatically excludes any integer $m \leq M$ possessing a prime divisor $p > 10^{10}$. It follows then that we can extend our search for allowable lengths of Barker sequences up to $n = 4M^2 = 2 \cdot 10^{30}$ by extending our search for Wieferich pairs (q, p) with $q < p$ for the case when $q > 10^5$. Table 3 exhibits the data for these new searches.

Table 3. More Wieferich pair searches, $p \equiv q \equiv 1 \bmod 4$.

q Range	p Range	Pairs	GHz-wks
$[10^6, 10^7]$	$[10^8, 7.5 \cdot 10^8]$	15274	50.4
$[10^5, 10^6]$	$[10^9, 7.5 \cdot 10^9]$	1684	76.4

The additional 16 958 ascending solid links found here give rise to another 39 797 descending solid links, and 41 434 new flimsy links. Our enlarged directed graph D now has 252 905 vertices, 387 444 solid edges, and 284 272 flimsy edges. Tarjan's algorithm produces just one additional cycle with this graph,

$$30\,109 \to 1\,128\,713 \to 268\,813\,277 \rightsquigarrow 2\,167\,849 \rightsquigarrow 30\,109,$$

but the corresponding value for m is far too large. However, running cycle augmentation on the examples of (5)–(9) with the larger M value produces several new candidates, and after final processing we find four additional plausible values for $m \leq 10^{15}/\sqrt{2}$:

$$217\,520\,382\,953\,549 = 13 \cdot 41 \cdot 2953 \cdot 138\,200\,401, \tag{15}$$

$$251\,651\,592\,370\,105 = 5 \cdot 193 \cdot 4877 \cdot 53\,471\,161, \tag{16}$$

$$485\,237\,777\,357\,917 = 29 \cdot 41 \cdot 2953 \cdot 138\,200\,401, \tag{17}$$

$$696\,441\,206\,924\,905 = 5 \cdot 13 \cdot 1601 \cdot 6\,692\,367\,337. \tag{18}$$

The large prime test of Corollary 2 excludes none of these, but Turyn's self-conjugacy test of Theorem 1 eliminates all but one possibility. For (16), use $r = 53\,471\,161$, $s = 4877^2 r^2$, and $j = 11\,890\,126$; for (17), select $r = 138\,200\,401$, $s = 29^2 \cdot 41^2 r^2$ and $j = 83\,230$; and for (18), choose $r = 6\,692\,367\,337$, $s = 13r^2$ and $j = 6$. We therefore conclude that if a Barker sequence of length $n > 13$ exists, then either

$$n = 4 \cdot 217\,520\,382\,953\,549^2 = 189\,260\,468\,001\,034\,441\,522\,766\,781\,604,$$

or $n > 2 \cdot 10^{30}$.

Despite their apparent scarcity, we expect that there exist infinitely many integers n satisfying the known constraints on the length of a Barker sequence. We present a heuristic argument for this assertion by estimating the number $G(x)$ of integers $m \le x$ for which $m = pq$ for primes p and q with $p < q$, $p \equiv q \equiv 1 \bmod 4$, both (p, q) and (q, p) are Wieferich prime pairs, and $q < 2p^2$. Each such integer m satisfies Corollary 2, Theorem 3, and Theorem 4. Evidently,

$$G(x) = \sum_{\substack{5 \le p \le \sqrt{x} \\ p \text{ prime} \\ p \equiv 1 \bmod 4}} \sum_{\substack{p \le q \le \min\{x/p, 2p^2\} \\ q \text{ prime} \\ q \equiv 1 \bmod 4 \\ q^{p-1} \equiv 1 \bmod p^2 \\ p^{q-1} \equiv 1 \bmod q^2}} 1.$$

By the Prime Number Theorem, the probability that a given integer z is prime approaches $1/\log z$ for large z, and it is well-known that primes which are congruent to 1 mod 4 have asymptotic density 1/2 in the space of primes. Further, we estimate the probability that (q, p) is a Wieferich prime pair, for a fixed prime p, is $1/p$, since $q^{p-1} \equiv ap + 1 \bmod p^2$ for some integer a satisfying $0 \le a < p$. Thus, we expect that

$$\begin{aligned} G(x) &\sim \frac{1}{4} \sum_{y=5}^{\sqrt{x}} \frac{1}{\log y} \sum_{z=y}^{\min\{x/y, 2y^2\}} \frac{1}{\log z} \cdot \frac{1}{yz} \\ &= \frac{1}{4} \left(\sum_{y=5}^{(x/2)^{1/3}} \sum_{z=y}^{2y^2} \frac{1}{yz \log y \log z} + \sum_{y=(x/2)^{1/3}}^{\sqrt{x}} \sum_{z=y}^{x/y} \frac{1}{yz \log y \log z} \right) \\ &\sim \frac{1}{4} \left(\int_5^{(x/2)^{1/3}} \int_y^{2y^2} \frac{dz\,dy}{yz \log y \log z} + \int_{(x/2)^{1/3}}^{\sqrt{x}} \int_y^{x/y} \frac{dz\,dy}{yz \log y \log z} \right). \end{aligned}$$

It is straightforward to check that both of the inner integrals above are bounded by a constant, so

$$G(x) \asymp \int_5^{\sqrt{x}} \frac{dy}{y \log y} \asymp \log\log x.$$

Turyn's self-conjugacy test of Theorem 1 will exclude some of the integers m counted by $G(x)$ when other values for r and s (besides $r = q$ and $s = 2q^2$) are employed. However, it seems reasonable to expect that this will affect our estimate only by a constant factor. We therefore conservatively expect that the existing restrictions on the length of a Barker sequence cannot eliminate $\Omega(\log\log x)$ integers $n \le x$ from consideration.

4.2. **Circulant Hadamard matrices.** In this problem, we choose $M = 10^{13}$, and begin in the same way by searching for Wieferich prime pairs (q, p) with $q < p$. This search is organized into a number of phases, as in the Barker sequence problem. In this computation, we restrict to the case where $p \equiv 3 \bmod 4$ or $q \equiv 3 \bmod 4$, since the case where $p \equiv q \equiv 1 \bmod 4$ was covered in the searches of section 4.1. Table 4 summarizes the organization and results of this search. Next, we compute all Wieferich prime pairs (q, p) with $10^7 > q > p$, and for each prime $q > 10^7$

appearing in a pair already found, we determine all pairs (q, p) with $p < \min\{q, M'\}$, with $M' = 10^7$. Applying a similar procedure for the construction of the sets V_k, we obtain a directed graph having 643 931 vertices, 1 732 862 solid edges (59 837 of them directed from a smaller prime to a larger one), and 1 729 116 flimsy edges. We then add 210 569 additional flimsy edges $q \rightsquigarrow 3$, one for each prime q not already linked to 3. This accounts for the possibility an integer $m \le M$ exists with the property that $F(m) = m^2/3 \ge m\varphi(m)$. The final directed graph D thus contains more than 3.6 million edges.

Table 4. Wieferich pair searches, $q < p$, p or $q \equiv 3 \bmod 4$.

q Bound	p Range	Pairs	GHz-wks
10^7	$[0, 10^7]$	36117	5.0
10^6	$[10^7, 10^8]$	7836	2.9
10^5	$[10^8, 10^9]$	867	3.4
10^4	$[10^9, 10^{10}]$	101	6.1
10^3	$[10^{10}, 10^{11}]$	11	9.6
10^2	$[10^{11}, 10^{12}]$	1	14.2
10	$[10^{12}, 10^{13}]$	0	28.8

Since the product of the twelve smallest odd primes exceeds M, we use the length restriction $\ell = 12$ in the cycle enumeration algorithm. Tarjan's algorithm runs in about 13 seconds on a 2.4 GHz Intel-based Apple computer, producing 461 653 distinct cycles, of which only 154 have a vertex product less than 10^{13}. The cycle augmenter then uses these cycles to generate (in about 9 seconds) a list of 7491 qualifying subgraphs of D. None of the integers m associated with these subgraphs has the property that $\prod_{q|m}(1 - 1/q)^{-1} \ge 3$, so we may assume that $F(m) = m^2$. After removing the integers that fail this condition, then inserting any allowable non-squarefree multiples of those that remain, we obtain a list of 2064 integers $m \le 10^{13}$ that satisfy Theorem 3. Turyn's self-conjugacy criterion of Theorem 1 eliminates at least 486 of these, leaving 1578 possible values for the order $n = 4m^2$ of a circulant Hadamard matrix with $4 < n \le 4 \cdot 10^{26}$. The smallest of these has $m = 11\,715$, as noted in [18, Cor. 4.5]. The second-smallest possibility, $m = 16\,401$, is not listed in [26, Thm. 3.2.8]; instead 82 005 is stated there as the next possible value for m larger than 11 715. However, we are not able to eliminate this number by using Theorem 1. In all, there are just ten permissible values of m with $4m^2 \le 10^{14}$:

$$\begin{aligned}
11\,715 &= 3 \cdot 5 \cdot 11 \cdot 71, & 16\,401 &= 3 \cdot 7 \cdot 11 \cdot 71,\\
82\,005 &= 3 \cdot 5 \cdot 7 \cdot 11 \cdot 71, & 550\,605 &= 3 \cdot 5 \cdot 11 \cdot 47 \cdot 71,\\
770\,847 &= 3 \cdot 7 \cdot 11 \cdot 47 \cdot 71, & 1\,806\,259 &= 7 \cdot 13 \cdot 23 \cdot 863,\\
2\,838\,407 &= 11 \cdot 13 \cdot 23 \cdot 863, & 3\,854\,235 &= 3 \cdot 5 \cdot 7 \cdot 11 \cdot 47 \cdot 71,\\
3\,877\,665 &= 3 \cdot 5 \cdot 11 \cdot 71 \cdot 331, & 4\,221\,305 &= 5 \cdot 11 \cdot 23 \cdot 47 \cdot 71.
\end{aligned}$$

For $n \le 10^{16}$, there are seventeen additional possibilities for m: 5 418 777, 5 428 731, 5 909 827, 8 515 221, 9 031 295, 9 047 885, 10 975 393, 12 663 915, 14 192 035, 16 256 331, 17 729 481, 19 868 849, 27 093 885, 27 143 655, 29 549 135, 32 926 179, and 42 576 105. The entire list of 1578 remaining values of $m \le 10^{13}$ is available at the author's web site [22].

5. Wieferich prime pairs

Since Wieferich prime pairs (q, p) arise in many problems in number theory, we describe our search for these primes in more detail here, and report on some results of particular interest. We first recall some prior searches. Owing to their historical interest, Wieferich pairs with $q = 2$ have received the most attention in earlier searches. Knauer and Richstein [16] recently completed a search for $p < 1.25 \cdot 10^{15}$ for this case, and a distributed computing project [32] now seeks to extend this bound.

For small values of the base q, in 1993 Montgomery [21] found all Wieferich pairs (q, p) with $q < 100$ and $p < 2^{32}$, checking composite bases q as well as prime ones. Keller and Richstein [15] in 2004 extended this search to $p < 10^{11}$ for primes $q < 1000$, and tested the bases $q = 3$ and $q = 5$ up to 10^{13}. More recently, Fischer [10] tested primes $p < 1.2 \cdot 10^{13}$ for bases $q \leq 61$, and checked at least as high as $p < 2.2 \cdot 10^{12}$ for other bases $q \leq 1050$. For larger prime values of q, Ernvall and Metsänkylä [9] in 1997 determined all Wieferich prime pairs (q, p) with $q < p < 10^6$.

Prior searches for Wieferich prime pairs employ some combination of three principal optimizations in their implementation. First, it is elementary that if (q, p) is a Wieferich prime pair with $p \neq 2$, then $q^{(p-1)/2} \equiv \pm 1 \bmod p^2$. Testing this condition clearly saves an iteration in the usual square-and-multiply algorithm for computing the residue of a power. Second, it is beneficial to store the remainder mod p^2 that is computed in each step of the square-and-multiply method in base p, since in this way one may guarantee that all intermediate results are less than p^2, rather than p^4. This allows one to use machine arithmetic, rather than big-integer software, for a much larger range of values for p. This tactic dates at least to D. H. Lehmer's 1981 search [17] for Wieferich pairs with base $q = 2$. Third, one can replace a division by a fixed quantity, such as p or p^2, with a suitable multiplication, followed by a division by a power of 2, a comparison, and (on average) one addition. This is advantageous on machines where multiplication is much faster than division, since dividing by a power of 2 can be implemented very efficiently by using a right bit shift. This technique is developed in [6], where it is called "steady-state division."

While we experimented with all three optimizations, the fastest method employed only the first of these, and relied on the highly optimized, assembly code implementation of the square-and-multiply operation in GMP [12] to compute residues of powers. This echos the decision made in [16] in the recent search for Wieferich pairs with base $q = 2$, but suggests that a careful implementation of the algorithm in assembly language using more of the enhancements may well be faster.

The searches described in section 4.2 extend the prior explorations by a considerable margin. In particular, Table 4 shows that the large search of Ernvall and Metsänkylä is extended by an order of magnitude in both dimensions, and Tables 2 and 3 extend prior searches for many bases when both primes are congruent to 1 mod 4. For the case of prime bases $q < 1000$, our computations produce five Wieferich pairs (q, p) that do not appear in the article of Keller and Richstein [15]:

$$\begin{gathered}(17, 478\,225\,523\,351),\ (157, 275\,318\,049\,829),\ (607, 22\,035\,814\,429),\\ (661, 462\,147\,547\,073),\ (953, 220\,564\,434\,997).\end{gathered} \tag{19}$$

(These pairs were also found by Fischer [10].) We remark that the third of these pairs, with $q = 607$, lies within the search range covered in [15], but was not reported there.

The first pair in (19), where $q = 17$, is of interest in the odd perfect number problem. In recent work on that question [23], Wieferich prime pairs in which the base q is a small Fermat prime are of some significance. (Recall that a Fermat prime is a prime number of the form $2^{2^m} + 1$.) Motivated by this application, we extended our searches for the case when q is a small Fermat prime by testing these against all primes $p < 10^{14}$. Table 5 summarizes these additional searches. No new Wieferich prime pairs were found in these computations. Note that for the case $q = 5$, we only needed to test primes $p \equiv 3 \bmod 4$, after the search reported in Table 2, so the CPU time required in that case is only about half that needed for $q = 3$.

Table 5. Additional Wieferich pair searches.

q	p Range	Pairs	GHz-wks
3	$[10^{13}, 10^{14}]$	0	117.2
5	$[10^{13}, 10^{14}]$	0	59.0
17	$[10^{12}, 10^{14}]$	0	122.9

Our searches did not reveal any additional double Wieferich prime pairs. Only seven such pairs are known:

$$(2, 1093),\ (3, 1\,006\,003),\ (5, 1\,645\,333\,507),\ (5, 188\,748\,146\,801),$$
$$(83, 4871),\ (911, 318\,917),\ (2903, 18\,787).$$

We also detected no Wieferich prime pairs (q, p) with $q < p$ that satisfy the stronger condition $q^{p-1} \equiv 1 \bmod p^k$ with $k > 2$. A large number of pairs with $q > p$ were found that satisfy a higher order Wieferich congruence; more than 84% of these have $p = 3$, 5, or 7. A few examples where $p > 3$ and either p or k is large are listed in Table 6.

Table 6. Some pairs (q, p) where $q^{p-1} \equiv 1 \bmod p^k$ with $k > 2$.

q	p	k
22 578 487	341 087	3
5 774 911	281	4
1 051 847	23	5
2 342 959	19	6
3 376 853	7	8
7 812 499	5	9

The Wieferich prime pairs (q, p) found in the searches that are summarized in Tables 2, 3, and 4, as well as some pairs that satisfy a higher-order Wieferich condition as in Table 6, are available at the author's web site [22].

Acknowledgements

I thank the Centre for Interdisciplinary Research in the Mathematical and Computational Sciences (IRMACS) at Simon Fraser University. I also thank the Department of Mathematics at the University of South Carolina for their hospitality during my visit during the 2008–09 academic year, when this research was conducted.

References

[1] R. H. Barker, *Group synchronizing of binary digital systems*, Communication Theory (London, 1952) (W. Jackson, ed.), Academic Press, New York, 1953, pp. 273–287.

[2] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, 1971. MR0282863 (44 #97)

[3] P. Borwein, E. Kaltofen, and M. J. Mossinghoff, *Irreducible polynomials and Barker sequences*, ACM Commun. Comput. Algebra **41** (2007), no. 3–4, 118–121. MR2404490

[4] P. Borwein and M. J. Mossinghoff, *Barker sequences and flat polynomials*, Number Theory and Polynomials (Bristol, U.K., 2006) (J. McKee and C. Smyth, eds.), London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, 2008, pp. 71–88.

[5] R. A. Brualdi, *A note on multipliers of difference sets*, J. Res. Nat. Bur. Standards Sect. B **69B** (1965), 87–89. MR0184868 (32 #2339)

[6] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), no. 217, 433–449. MR1372002 (97c:11004)

[7] S. Eliahou and M. Kervaire, *Barker sequences and difference sets*, Enseign. Math. (2) **38** (1992), no. 3-4, 345–382. Corrigendum, Enseign. Math. (2) **40** (1994), no. 1–2, 109–111. MR1189012 (93i:11018)

[8] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory Ser. A **55** (1990), no. 1, 49–59. MR1070014 (91i:11020)

[9] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. **66** (1997), no. 219, 1353–1365. MR1408373 (97i:11003)

[10] R. Fischer, *Fermat quotients.* http://www.fermatquotient.com/FermatQuotienten.

[11] M. L. Fredman, B. Saffari, and B. Smith, *Polynômes réciproques: conjecture d'Erdős en norme L^4, taille des autocorrélations et inexistence des codes de Barker*, C. R. Acad. Sci. Paris Sér. I Math. **308** (1989), no. 15, 461–464. MR994692 (90c:42004)

[12] *GMP: The GNU multiple precision arithmetic library.* http://www.swox.com/gmp.

[13] A. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714, 591, 416, 091, 389, Trans. Amer. Math. Soc. **306** (1988), no. 1, 329–359. MR0927694 (89g:11025)

[14] J. Jedwab and S. Lloyd, *A note on the nonexistence of Barker sequences*, Des. Codes Cryptogr. **2** (1992), no. 1, 93–97. MR1157481 (93e:11032)

[15] W. Keller and J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. **74** (2005), no. 250, 927–936. MR2114655 (2005i:11004)

[16] J. Knauer and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), no. 251, 1559–1563. MR2137018 (2006a:11006)

[17] D. H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. **36** (1981), no. 153, 289–290. MR595064 (82e:10004)

[18] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), no. 2, 171–188. MR2211106 (2007g:05023)

[19] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195. MR2076124 (2005f:11051)

[20] ———, *A class number free criterion for Catalan's conjecture*, J. Number Theory **99** (2003), no. 2, 225–231. MR1968450 (2004b:11040)

[21] P. L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61** (1993), no. 203, 361–363. MR1182246 (94d:11003)

[22] M. J. Mossinghoff, *Wieferich prime pairs, Barker sequences, and circulant Hadamard matrices*, 2009. http://www.cecm.sfu.ca/∼mjm/WieferichBarker.

[23] P. P. Nielsen, *Odd perfect numbers have at least nine distinct prime factors*, Math. Comp. **76** (2007), no. 260, 2109–2126.

[24] H. J. Ryser, *Combinatorial Mathematics*, Carus Math. Monogr., vol. 14, Math. Assoc. Amer., 1963. MR0150048 (27 #51)

[25] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), no. 4, 929–952. MR1671453 (2000a:05042)

[26] ———, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Math., vol. 1797, Springer-Verlag, 2002. MR1943360 (2004a:05028)

[27] R. Tarjan, *Enumeration of the elementary circuits of a directed graph*, SIAM J. Comput. **2** (1973), 211–216. MR0325448 (48 #3795)

[28] R. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346. MR0179098 (31 #3349)

[29] ______, *Sequences with small correlation*, Error Correcting Codes (Madison, WI, 1968) (H. B. Mann, ed.), J. Wiley & Sons, New York, 1968, pp. 195–228. MR0242566 (39 #3897)

[30] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399. MR0125026 (23 #A2333)

[31] A. Wieferich, *Zum letzten Fermat'schen theorem*, J. Reine Angew. Math. **136** (1909), 293–302.

[32] *Wieferich@Home*, 2009. http://www.elmath.org.

Department of Mathematics, Box 6996, Davidson College, Davidson, North Carolina 28035-6996

E-mail address: mimossinghoff@davidson.edu