DOUBLE WIEFERICH PAIRS AND CIRCULANT HADAMARD MATRICES

BROOKE LOGAN AND MICHAEL J. MOSSINGHOFF

ABSTRACT. We show that all but 4489 integers n with $4 < n \leq 4 \cdot 10^{30}$ cannot occur as the order of a circulant Hadamard matrix. Our algorithm allows us to search 10000 times farther than prior efforts, while substantially reducing memory requirements. The principal improvement over prior methods involves the incorporation of a separate search for double Wieferich prime pairs $\{p, q\}$, which have the property that $p^{q-1} \equiv 1 \bmod q^2$ and $q^{p-1} \equiv 1 \bmod p^2$.

1. INTRODUCTION

An $n \times n$ matrix H, each of whose entries is ± 1, is a *Hadamard matrix* if $HH^T = nI_n$, that is, if its rows are mutually orthogonal. A matrix is *circulant* if each row after the first one is a cyclic shift to the right by one position of the prior row. The matrix

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

has both properties, but no circulant Hadamard matrices of order $n > 4$ are known. The well-known *circulant Hadamard matrix conjecture* asserts that none of higher order exists. This problem is more than a half-century old, dating at least to the monograph of Ryser [14].

A number of necessary conditions are known for an integer $n > 4$ to be the order of a circulant Hadamard matrix. Ryser noted that n must be a square, and subsequently Turyn [19,20] showed that n must have the form $4u^2$ with u odd and not a prime power, and further that $u \geq 55$. In 1999, Schmidt [15] raised this bound to $u \geq 165$, and in 2002 [16] found that only two additional values of $u > 1$ could not be disqualified up to $5 \cdot 10^{9/2}$:

2010 *Mathematics Subject Classification.* Primary: 05B20, 15B34; Secondary: 05-04, 05B10, 11A41.

Key words and phrases. Circulant Hadamard matrix, Wieferich prime pair.

Research of M. J. Mossinghoff was partially supported by a grant from the Simons Foundation (#210069).

$u = 11715$ and $u = 82005$. In 2005, Leung and Schmidt [8] improved the lower bound to $u \geq 11715$. These results employed some very restrictive algebraic conditions on u arising from their field descent method [8, 16]. These conditions are described in Section 2, but they involve a requirement that among the prime divisors of u there must exist a number of *Wieferich prime pairs*, which are pairs (q, p) with the property that $q^{p-1} \equiv 1 \bmod p^2$. Articles by P. Borwein and the second author [1, 12] exploited this structure to construct all integers $1 < u \leq 10^{13}$ for which $n = 4u^2$ could not be excluded as the order of a circulant Hadamard matrix by using the known restrictions. These searches produced only 1453 different permissible integers using restrictions known in 2009, and this was reduced to 1371 possibilities by employing three additional algebraic restrictions found by Leung and Schmidt in 2012 [9]. More recently, a powerful new restriction developed by Leung and Schmidt [10] reduced this number to 882 possible values.

In those prior searches, the most computationally expensive case checked for the possibility that $u = pq$ for distinct odd primes p and q. This could occur only when $\{p, q\}$ form a *double Wieferich prime pair*, that is, when both (q, p) and (p, q) are Wieferich prime pairs. In this article, we employ a separate and more efficient search for double Wieferich prime pairs, using the method of Keller and Richstein [7]. With this case handled separately, other cases can assume additional information on u—in particular, the presence of at least three distinct prime factors. This allows for a sizable increase in the space we can search, while substantially decreasing the overall memory requirement. Using this strategy, we magnify the bound on u by a factor of 100, and thus increase the bound on possible orders of circulant Hadamard matrices by a factor of 10^4. We find that all but 4489 integers n with $4 < n \leq 4 \cdot 10^{30}$ can be eliminated as the order of such a matrix. The details of our search strategy appear in Section 3, and we summarize its results in Section 4. Some brief remarks on a special case of the circulant Hadamard matrix conjecture known as the *Barker sequence problem*, which was the primary focus of [1, 12], appear in Section 5.

The smallest integer $n > 4$ that cannot be excluded as a possible order of a circulant Hadamard matrix remains the example of Leung and Schmidt, $n = 4 \cdot 11715^2 = 548\,964\,900$.

2. Restrictions on circulant Hadamard matrices

We summarize a number of known algebraic restrictions on the order $n = 4u^2$ of a circulant Hadamard matrix when $u > 1$. We recall that Turyn showed that u must be odd, and must have at least two distinct prime divisors. Turyn [19] also established a more complicated criterion known as the *self-conjugacy test*. For this, given two integers a and b, we say a is

semiprimitive modulo b if there exists an integer j such that $a^j \equiv -1 \bmod b$. We say an integer r is *self-conjugate* modulo an integer s if each prime divisor p of r is semiprimitive mod s_p, where s_p denotes the largest divisor of s not divisible by p. Turyn proved the following theorem.

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

Jedwab and Lloyd [6] noted a useful special case of this, obtained by selecting $r = p^k$ for an odd prime p and $s = 2p^{2k}$.

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

For the next two tests, we require some definitions. Let $\mathcal{D}(t)$ denote the set of prime divisors of the integer t. For a positive integer m and a prime q, let

$$m_q = \begin{cases} \displaystyle\prod_{p \in \mathcal{D}(m) \setminus \{q\}} p & \text{if } m \text{ is odd or } q = 2, \\ \displaystyle 2 \prod_{p \in \mathcal{D}(m) \setminus \{q\}} p & \text{otherwise.} \end{cases}$$

Next, let $\mathrm{ord}_s(t)$ denote the order of t in the multiplicative group $(\mathbb{Z}/s\mathbb{Z})^*$, and for a prime p let $\nu_p(t)$ denote the largest integer k such that $p^k \mid t$ but $p^{k+1} \nmid t$. For positive integers m and n and a prime p, define $b(p, m, n)$ by

$$b(p, m, n) = \begin{cases} \displaystyle\max_{q \in \mathcal{D}(n) \setminus \{2\}} \left\{ \nu_2(q^2 - 1) + \nu_2(\mathrm{ord}_{m_q}(q)) - 1 \right\} & \text{if } p = 2, \\ \displaystyle\max_{q \in \mathcal{D}(n) \setminus \{p\}} \left\{ \nu_p(q^{p-1} - 1) + \nu_p(\mathrm{ord}_{m_q}(q)) \right\} & \text{if } p > 2, \end{cases}$$

with the convention that $b(2, m, 2^k) = 2$ and $b(p, m, p^k) = 1$ for an odd prime p and an integer $k \geq 0$. Then define $F(m, n)$ by

$$F(m, n) = \gcd\left(m, \prod_{p \in \mathcal{D}(m)} p^{b(p,m,n)} \right).$$

Leung and Schmidt [8] established the following restriction, which we call the *F-test*. Here, $\varphi(\cdot)$ denotes Euler's totient function.

Restriction 3. *If $n = 4u^2$ is the order of a circulant Hadamard matrix, then $u\varphi(u) \leq F(u^2, u)$.*

Next is a bound of Leung and Schmidt from [9] that also depends on the function $F(m, n)$. We cite their result here only as it applies to the circulant Hadamard matrix problem.

Restriction 4. *If $n = 4u^2$ is the order of a circulant Hadamard matrix, and m and w are positive integers with $m \mid u$, $w \mid n$, and m is self-conjugate modulo n/w, then $n\varphi(F(n/w, u^2/m^2)) \leq w^2 F(n/w, u^2/m^2)^2$.*

The article [9] of Leung and Schmidt established two additional restrictions involving self-conjugacy, which apply only in certain special cases. One requires that u have a particularly large prime-power divisor, although not as large as that needed in Restriction 2.

Restriction 5. *Suppose that $n = 4u^2$ is the order of a circulant Hadamard matrix, let p be an odd prime dividing u, let $a = \nu_p(u)$, and suppose that $p^{2a} > 2u$. Further, let r be a divisor of $m = u/p^a$, with r self-conjugate modulo p, and suppose that $q_1, \ldots, q_k$ are the prime divisors of m/r. Then* $\gcd(\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_k)) \leq m^2/r^2$.

The last restriction from [9] applies when u is composed entirely of primes that satisfy a simple congruence condition.

Restriction 6. *Let u be an integer whose prime divisors are all congruent to 3 mod 4. Let p be one of these divisors, and suppose that w is a divisor of u that is self-conjugate modulo p. Let $q_1, \ldots, q_k$ be the prime divisors, excluding p, of u/w. If $u = w$ or* $\gcd(\mathrm{ord}_p(q_1), \ldots, \mathrm{ord}_p(q_k)) \leq u^2/w^2$, *then no circulant Hadamard matrix of order $4u^2$ exists.*

Finally, Leung and Schmidt [10] recently determined an additional algebraic restriction on the order of a circulant Hadamard matrix. For positive integers x and y, let $\omega(x, y)$ denote the largest divisor of x that is relatively prime to y.

Restriction 7. *Let u be an odd integer, let $d \mid u$ so that* $\gcd(d, u/d) = 1$, *and let p be a prime divisor of u/d with the property that $2u^2\varphi(d^2) < p\varphi(u^2)$. Let a be the multiplicity of p in u/d, let m be a divisor of u with $p^a \mid m$ such that $\nu_p(\mathrm{ord}_{p^{2a}}(q)) > \nu_p(\mathrm{ord}_{\omega(u/d,q)}(q))$ for every prime divisor $q \neq p$ of u. Let t be an integer satisfying* $\gcd(t, u/d) = 1$ *and for every prime divisor q of u/m there is an integer s_q with $q^{s_q} \equiv t \bmod \omega(u^2/d^2, q)$. Let S be the set of prime divisors of $u/(dp^a)$, and set*

$$S' = \begin{cases} \{s \in S : \nu_2(\mathrm{ord}_s(t)) = \nu_2(\mathrm{ord}_p(t))\}, & \text{if } 2 \mid \mathrm{ord}_p(t), \\ \emptyset, & \text{if } 2 \nmid \mathrm{ord}_p(t). \end{cases}$$

In addition, if u/m is a prime power q^b then set $S' = S' \cup \{q\}$. For $s \in S \backslash S'$, set $f_s = \min\{\mathrm{ord}_{p^s}(t)/\mathrm{ord}_p(t), (s-1)/2\}$. If

$$\mathrm{ord}_p(t) > \frac{u^4}{m^4} \max\left\{ \left\{ \frac{2m^2}{u^2} \right\} \bigcup \left\{ \frac{s-1}{f_s(s-f_s)} : s \in S \backslash S' \right\} \right\}, \qquad (1)$$

then no circulant Hadamard matrix of order $4u^2$ exists.

Our strategy for selecting parameters when applying Restriction 7 is discussed in Section 4.

3. Search strategy

Our strategy is similar to the one employed in [1]. We describe the method briefly here, highlighting the improvements, and refer the reader to [1] for additional details.

We wish to construct all odd integers $u \leq U = 10^{15}$ with at least two distinct prime divisors so that u satisfies the F-test of Restriction 3. By Restriction 2, we need only consider prime divisors up to $V := (2U^2)^{1/3} = 2^{1/3} \cdot 10^{10}$. Since u is odd and not a prime power, and $\nu_p(q^{p-1} - 1) \geq 1$ for distinct primes p and q, we see that $b(p, u^2, u) \geq 1$ for each prime $p \mid u$, and consequently $F(u^2, u)$ has exactly the same prime divisors as u. If $F(u^2, u) \leq u^2/p$ for some prime $p \mid u$, and $F(u^2, u) \geq u\varphi(u)$, then it follows that $p \leq \prod_{q|u}(1 - 1/q)^{-1}$, and this latter quantity is at most $3.446\ldots$ for $u \leq U$ (attained when u is the product of all odd primes up to 41). Thus, if an integer $u \leq U$ passes the F-test, then either $F(u^2, u) = u^2$, or possibly $F(u^2, u) = u^2/3$ when $3 \mid u$.

Since $F(u^2, u)$ depends only on the squarefree part of u, we consider the squarefree case first. If $p \mid u$ for a prime $p \geq 5$, we require that $b(p, u^2, u) \geq 2$, and it follows that at least one of the following two conditions must hold: (i) there exists a prime $q \mid u$ so that (q, p) is a Wieferich prime pair, or (ii) there exists a prime $q \mid u$ so that $p \mid \mathrm{ord}_{u_q}(q)$. The second case requires the existence of another prime $r \mid u$ so that $p \mid (r - 1)$.

We search for permissible values of $u \leq U$ by creating a large directed graph $D(U)$, whose vertices are a subset of the primes up to U, and which has two types of edges. A *solid edge* $q \to p$ links q to p for each Wieferich prime pair (q, p), and a *flimsy edge* $r \rightsquigarrow p$ connects r to p if $p \mid (r - 1)$. A flimsy edge is also added from each prime $p > 3$ in $D(U)$ to 3 to account for the looser restriction at this prime. Candidates for integers u that pass the F-test then correspond to induced subgraphs of $D(U)$ in which each vertex has positive indegree. Our method first searches for cycles of length at most 12 in this graph, since the product of the smallest 13 odd primes exceeds U. For each such cycle, we then determine all induced subgraphs of $D(U)$ containing this cycle, and additional edges that flow outward from the vertices in the cycle, with the property that the product of the vertices in the subgraph is at most U. Each flimsy edge in such a subgraph is then tested to ensure that the F-test is indeed satisfied, since the order condition is stronger than the simple division constraint of the construction, and because F must be evaluated at each candidate value u to determine the requirement at the prime 3. For each permissible value u discovered, we also construct all non-squarefree multiples of u having the

same prime factors as u that pass the F-test and remain below the bound of U, by observing the values of $b(p, u^2, u)$ for $p \mid u$.

Since a flimsy edge $r \rightsquigarrow p$ connects a prime r to a smaller prime p, every cycle in $D(U)$ must contain a solid edge $q \to p$ with $q < p$. We call such a pair an *ascending Wieferich pair*. These are rare, and most of our computation is devoted to searches for these pairs. In prior work, for each prime $q < U$ we tested every prime $p \leq \min\{U/q, V\}$ for a possible ascending Wieferich pair (q, p). However, many of these tests are unnecessary. An integer u of the form $u = pq$ passes the F-test only if $\{p, q\}$ is a double Wieferich prime pair, since a flimsy link requires the presence of a third prime r distinct from p and q. In the current method, we search for these double Wieferich pairs separately, using a more efficient method. For this, we employ a result first noted by Worms de Romilly in 1901 [22] (see also [7] for a generalization to higher-power congruences).

Proposition 1. *Let a be a primitive root of a prime q, and let $b \equiv a^q \bmod q^2$. Then all solutions to $x^{q-1} \equiv 1 \bmod q^2$ are given by $b^k \bmod q^2$, for $0 \leq k \leq q-2$.*

Following Keller and Richstein [7], we use this result to search for double Wieferich prime pairs $\{p, q\}$ by implementing the following algorithm.

Step 1. For each odd prime $q \leq \sqrt{U}$, perform Step 2.

Step 2. Compute a primitive root a mod q, and set $b \equiv a^q \bmod q^2$.

Step 3. For each power b^k mod q^2 with $0 \leq k \leq q-2$, perform Step 4.

Step 4. For each odd integer p with $q < p < \min\{U/q, V\}$ and $p \equiv b^k \bmod q^2$, test if p is prime. By Proposition 1, for each prime p discovered, the pair (p, q) is automatically a *descending* Wieferich pair, so test if $q^{p-1} \equiv 1 \bmod p^2$. Print $\{p, q\}$ if this holds.

For a fixed prime q, we need only search $q-1$ of the residue classes mod q^2, so this procedure speeds the search for double Wieferich prime pairs by approximately a factor of q. We remark that for efficiency we employ a simple pseudoprime test in Step 4 (one iteration of Miller-Rabin with a fixed base, after a gcd computation checks for divisibility by any of the first ten odd primes), and verify primality of p only in the pairs $\{p, q\}$ reported.

Next, we search for additional ascending pairs (q, p) that are required for our graph $D(U)$. Let q be an odd prime with $q \leq \sqrt{U}$. We wish to determine all primes p with $q < p \leq V$ which may appear in the construction of an integer $u \leq U$ that passes the F-test, with the knowledge that $\{p, q\}$ is not a double Wieferich prime pair. We consider three cases.

(i) If $p \rightsquigarrow q$, then $q \mid (p-1)$, and a third prime $r \geq 3$ must be present as well in u for the flimsy link to be valid, so we need only search

primes $p \equiv 1 \bmod q$ with $q < p \leq \min\{U/3q, V\}$ if $q > 3$ and $q < p \leq \min\{U/15, V\}$ if $q = 3$.

(ii) If $q \to p$ augments another cycle, then we may account for the primes in the cycle when computing an upper bound for p. From the results of [1], we know that the cycle with minimal vertex product is $3 \to 11 \to 71 \to 3$, with value $3 \cdot 11 \cdot 71 = 2343$. We consider three cases.

- If $q = 3$, 11, or 71, then we need to check primes p satisfying $p \leq \min\{U/2343, V\}$. Let R_1 denote the set of primes p found here for which $q \to p$ is an ascending Wieferich pair, and let $R_2 = \{5, 7, 47\}$, which are the primes involved in either descending Wieferich pairs or flimsy links beginning from 3, 11, or 71. (These links are $11 \rightsquigarrow 5$, $71 \rightsquigarrow 5$, $71 \rightsquigarrow 7$, and $71 \to 47$.) Let $R = R_1 \cup R_2$.
- If $q \in R$ then we search for primes $p > q$ which satisfy $p \leq \min\{U/2343q, V\}$.
- For all other primes q, we know that an ascending pair $q \to p$ cannot connect directly to the smallest cycle, so either this link attaches to another cycle, or it attaches to the minimal cycle, but indirectly, with at least one other prime s as an intermediary. Certainly $s \geq 5$. Since the second-best cycle is $13 \to 863 \rightsquigarrow 23 \to 13$, whose value of 258037 is larger than $5 \cdot 2343 = 11715$, we can search for primes $p > q$ satisfying $p \leq \min\{U/11715q, V\}$.

(iii) If $q \to p$ forms one edge of a cycle, then there must exist at least one additional prime r linking to q in the cycle. We consider two cases.

- If $r > q$, then we need to test primes p satisfying $q < p \leq \min\{U/(q \cdot \mathrm{succ}(q)), V\}$, where $\mathrm{succ}(q)$ denotes the smallest prime larger than q.
- If $r < q$, then (r, q) is also an ascending Wieferich pair. Assuming that we are testing the primes q in ascending order, we can look up the smallest prime r for which (r, q) is an ascending Wieferich pair. If such an r exists, we test primes p in the range $q < p \leq \min\{U/qr, V\}$. In practice, we test blocks of primes concurrently using a cluster, so processing of prior primes is not always complete when a search is being performed for a particular prime q. Because of this we first complete searches for the first t odd primes. Then for larger primes q, we need to test primes p in the range $q < p \leq \min\{U/p_{t+1}q, V\}$, where p_{t+1} denotes the $(t+1)$st odd prime, if no ascending pair (r, q) is known at the time of the search. We can select t so that this constraint is stronger than that of case (ii).

For each prime q then we perform the search indicated in case (i), and the search corresponding to the weakest constraint from cases (ii) and (iii).

The primes 3, 7, and 71 are considered first, then the primes in the set R constructed during this search, and then the remaining odd primes $q \leq \sqrt{U}$.

Once the search for ascending Wieferich pairs is complete, we search for descending pairs and flimsy links by using a strategy somewhat more refined than that employed in [1, 12]. First, for each prime p appearing in an ascending pair $q \to p$, we find all odd primes $r < p$ so that (p, r) is a descending Wieferich pair and add the solid link $p \to r$ to $D(U)$. We also compute the prime factors of $p-1$ and add a flimsy link from p to any such odd prime factor r, provided there is not already a solid link from p to r. For each such new link $p \to r$ or $p \rightsquigarrow r$ discovered, we repeat this process on the prime r if it has not yet been explored. This process continues until no new primes appear.

4. Results

4.1. **Circulant Hadamard matrices.** Our search was implemented in C++, using GMP [4] for arithmetic with large integers. With $U = 10^{15}$, we find that $R_1 = \{331, 1006003\}$ in our construction, arising from $3 \to 1006003$ and $71 \to 331$. We construct the graph $D(U)$ having 10020 vertices, 21385 Wieferich prime pairs (4501 of them ascending), 16348 flimsy links arising from the divisibility constraint, and an additional 2603 flimsy links to the prime 3 to allow for the possibility that $F(u^2, u) = u^2/3$ in the F-test. This graph is significantly smaller than the graph constructed in [12] using $U = 10^{13}$, owing to our more efficient search strategy in using a separate algorithm for the case of double Wieferich prime pairs, and to our more refined search strategy for the various kinds of links. The graph in [12] had 643931 vertices, 1732862 solid edges, and 1939685 flimsy edges, and so required more than 91 times the storage using an adjacency list representation for its graph.

Tarjan's algorithm [18] for enumerating cycles in a directed graph detects 402 different cycles in $D(U)$ with vertex product $u \leq U$. The cycle augmenter produces 7021 permissible induced subgraphs of $D(U)$ containing one of these cycles. We then verify the F-test for each corresponding integer u, checking each required flimsy link and testing if $\prod_{q|u}(1-1/q)^{-1} \geq 3$ when $3 \mid u$. At the same time, we test if any non-squarefree multiples of permissible values u also pass the F-test. This produces 8204 positive integers $u \leq 10^{15}$ that pass both Restrictions 2 and 3.

These values are then subjected to Turyn's self-conjugacy test of Restriction 1, followed by the four criteria of Leung and Schmidt. We apply Restrictions 5 and 6 before Restriction 4 since the last is more time-consuming. In Restriction 7, for each divisor d of u satisfying $\gcd(d, u/d) = 1$, we consider each prime divisor p of u/d, ordered from largest to smallest. We then take m to be as large as possible relative to this choice. Since the

TABLE 1. Effect of Restrictions 1, 4, 5, 6, and 7 for $U = 10^{15}$.

$\Omega(u)$	Initial Number	Exclusions from Restrictions: Res 1	Res 5	Res 6	Res 4	Res 7	Admissible Number
2	5	5	–	–	–	–	0
3	60	51	0	0	0	5	4
4	312	203	5	3	10	24	67
5	1005	361	16	17	31	167	413
6	2019	418	8	22	42	463	1066
7	2425	269	3	25	27	701	1400
8	1637	100	0	6	8	528	995
9	628	18	0	0	0	169	441
10	109	1	0	0	0	9	99
11	4	0	0	0	0	0	4
Total	8204	1426	32	73	118	2066	4489

right side of (1) is at least $2u^2/m^2$, we can reject the current choice of p if $(p-1)/2 \leq u^2/m^2$. In almost all cases that survive this filter, we find that u/m is a prime power, which simplifies our choice of t. When $u/m = q^b$, we choose $t = q$ if $q \nmid u/d$, and if $q \mid u/d$, then we select t so that $t \equiv 1 \bmod q$ and $t \equiv q \bmod \omega(u^2/d^2, q)$. This strategy lets us eliminate 2065 of the 6555 values of u that survived the other restrictions. Only five of the possible values of u force a choice of m so that u/m has more than one factor, and Restriction 7 allows us to handle one of these: $u = 3639009138645 = 3 \cdot 5 \cdot 44963 \cdot 5395561$, by choosing $d = 15$, $p = 44963$, $m = u/d$, and $t = 44234923246041944760450$. Table 1 exhibits the number of values u that were eliminated by each of these tests, organized by the number of prime factors $\Omega(u)$ of u, counting multiplicity.

The five smallest integers $u > 1$ that survive all known necessary conditions for $n = 4u^2$ to be the order of a circulant Hadamard matrix remain $11715 = 3 \cdot 5 \cdot 11 \cdot 71$, $82005 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 71$, $550605 = 3 \cdot 5 \cdot 11 \cdot 47 \cdot 71$, $3854235 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 47 \cdot 71$, and $3877665 = 3 \cdot 5 \cdot 11 \cdot 71 \cdot 331$. The five smallest permissible values $u > 10^{13}$ determined here are

$$10010975913705 = 3 \cdot 5 \cdot 13 \cdot 23 \cdot 83 \cdot 4871 \cdot 5521,$$
$$10114065558733 = 37 \cdot 83 \cdot 293 \cdot 821 \cdot 13691,$$
$$10133892169345 = 5 \cdot 7 \cdot 7 \cdot 19 \cdot 43 \cdot 103 \cdot 491531,$$
$$10163608060697 = 7 \cdot 13 \cdot 23 \cdot 467 \cdot 863 \cdot 12049,$$
$$10171384404951 = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 71 \cdot 307 \cdot 331 \cdot 359,$$

and the five largest possible $u < 10^{15}$ are

$$992395041021485 = 5 \cdot 23 \cdot 41 \cdot 83 \cdot 487 \cdot 1069 \cdot 4871,$$
$$994687636227489 = 3 \cdot 3 \cdot 41 \cdot 83 \cdot 487 \cdot 4871 \cdot 13691,$$
$$994985827355325 = 3 \cdot 5 \cdot 5 \cdot 13 \cdot 17 \cdot 23 \cdot 251 \cdot 863 \cdot 12049,$$
$$995017496776329 = 3 \cdot 13 \cdot 23 \cdot 29 \cdot 41 \cdot 83 \cdot 821 \cdot 13691,$$
$$999646398756005 = 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 467 \cdot 743 \cdot 863.$$

All 4489 permissible values of $u < 10^{15}$ are available at the website [13].

4.2. **Double Wieferich prime pairs.** Our search detects five double Wieferich prime pairs $\{p, q\}$ with p and q odd, $pq \le U = 10^{15}$, and $\max\{p, q\} \le V = 2^{1/3} \cdot 10^{10}$: $\{3, 1006003\}$, $\{5, 1645333507\}$, $\{83, 4871\}$, $\{911, 318917\}$, and $\{2903, 18787\}$. All of these had been found in prior searches, respectively by Brillhart, Tonascia, and Weinberger [2], Montgomery [11], Aaltonen (see [5]), and the last two are credited to Mignotte and Roy in an unpublished manuscript of 1992 (see for instance [3]). Only one other double Wieferich pair is known where p and q are both odd: $\{5, 188748146801\}$. It lies outside our search range, and was found by Keller and Richstein [7]. (Keller and Richstein searched systematically for double Wieferich pairs having $q < 10^6$ and $p < \max\{10^{11}, q^2\}$; their example arose in a separate search for ascending Wieferich pairs with base 5.)

5. Barker sequences

A *Barker sequence* is a finite sequence $a_1, \ldots, a_n$, each term ± 1, for which $\left|\sum_{i=1}^{n-k} a_i a_{i+k}\right| \le 1$ for $0 < k < n$. The longest known Barker sequence has length 13, and it is widely conjectured that no longer Barker sequences exist. This has been established for sequences with odd length [17,21], but the even case remains open. It is well known that this problem would be settled if one could show that no additional circulant Hadamard matrices exist, since every Barker sequence with even length n can be used to create such a matrix of order n. In [1] it was shown that only one integer n with $13 < n \le 4 \cdot 10^{33}$ survives Restrictions 1–6, plus an additional restriction that applies to Barker sequences of even length: if $p \mid u$ then $p \equiv 1 \bmod 4$. This value is $n = 4u_0^2$, where

$$u_0 = 31540455528264605 = 5 \cdot 13 \cdot 29 \cdot 41 \cdot 2953 \cdot 138200401.$$

Another 237806 candidate lengths n with $4 \cdot 10^{33} < n \le 10^{100}$ were also identified in [1], but without certifying if that list was complete in this range. As reported in [10], the anti-field-descent test (Restriction 7) eliminates $4u_0^2$, along with more than 96.5% of the other 237806 known candidates; the 8125 surviving permissible values for u from that list can be found at [13]. The

smallest known integer that survives all known restrictions on the length of a Barker sequence, including Restriction 7, is now $n = 4u_1^2$, where

$$\begin{aligned} u_1 &= 1980430483001226429873804 1 \\ &= 30109 \cdot 1128713 \cdot 2167849 \cdot 268813277. \end{aligned} \tag{2}$$

We remark that u_1 has 26 digits and $4u_1^2$ has 52 digits. It should be noted however that because the method of [1] established completeness only up to $U = 10^{16.5}$, it is possible that $4u_1^2$ is not the smallest integer that survives all of the known restrictions on the length of a Barker sequence. This method of this paper may be used to extend the validated range in the Barker sequence problem from the present limit of $U = 10^{16.5}$ to perhaps 10^{19} or 10^{20} at this time, but achieving $U = 2 \cdot 10^{25}$ to reach (2) seems out of reach at present. We leave this to future research.

ACKNOWLEDGEMENTS

We thank the Institute for Computational and Experimental Research in Mathematics (ICERM) at Brown University, and the Summer@ICERM 2014 Research Experiences for Undergraduates program, where this research was conducted. We also thank the Center for Computation and Visualization at Brown University, the Centre for Interdisciplinary Research in the Mathematical and Computational Sciences (IRMACS) at Simon Fraser University, and WestGrid, the high performance computing consortium and subdivision of Compute Canada, for computational resources.

REFERENCES

[1] P. Borwein and M. J. Mossinghoff, *Wieferich pairs and Barker sequences, II*, LMS J. Comput. Math. **17** (2014), no. 1, 24–32. MR3230855

[2] J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, London, 1971, pp. 213–222. MR0314736 (47 #3288)

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

[4] T. Granlund and the GMP development team, *GMP: The GNU multiple precision arithmetic library*, ver. 4.3.1, 2009. https://gmplib.org.

[5] K. Inkeri, *On Catalan's conjecture*, J. Number Theory **34** (1990), no. 2, 142–152. MR1042488 (91e:11030)

[6] 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)

[7] 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)

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

[9] ———, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64** (2012), no. 1-2, 143–151. MR2914407

[10] ———, *The anti-field-descent method* (2015). Preprint.

[11] 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)
[12] M. J. Mossinghoff, *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. **53** (2009), no. 3, 149–163. MR2545689 (2011c:11039)
[13] ———, *Wieferich prime pairs, Barker sequences, and circulant Hadamard matrices*, 2015. http://www.cecm.sfu.ca/~mjm/WieferichBarker.
[14] H. J. Ryser, *Combinatorial Mathematics*, Carus Math. Monogr., vol. 14, Math. Assoc. Amer., 1963. MR0150048 (27 #51)
[15] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), no. 4, 929–952. MR1671453 (2000a:05042)
[16] ———, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Math., vol. 1797, Springer, 2002. MR1943360 (2004a:05028)
[17] K.-U. Schmidt and J. Willms, *Barker sequences of odd length*, Des. Codes Cryptogr., 6 pp. Published online June 16, 2015. DOI 10.1007/s10623-015-0104-4.
[18] R. Tarjan, *Enumeration of the elementary circuits of a directed graph*, SIAM J. Comput. **2** (1973), 211–216. MR0325448 (48 #3795)
[19] R. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346. MR0179098 (31 #3349)
[20] ———, *Sequences with small correlation*, Error Correcting Codes (Madison, WI, 1968), J. Wiley, New York, 1968, pp. 195–228. MR0242566 (39 #3897)
[21] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399. MR0125026 (23 #A2333)
[22] A. S. Worms de Romilly, *Équation* $a^{p-1} = 1 +$ *mult.* p^2, L'Intermédiare des Math. **8** (1901), 214–215.

Department of Mathematics, Rowan University, Glassboro, NJ 08028 USA
E-mail address: brooke.logan@rutgers.edu

Department of Mathematics and Computer Science, Davidson College, Davidson, NC 28035-6996 USA
E-mail address: mimossinghoff@davidson.edu