Advances in Possible Orders of Circulant Hadamard Matrices, and Sequences with Large Merit Factor

Jason Hu\(^1\)  Brooke Logan\(^2\)

\(^1\)Department of Mathematics  
University of California, Berkeley

\(^2\)Department of Mathematics  
Rowan University

August 7, 2014
Outline

Introduction
   Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
   Restrictions on n
   Ascending Wieferich Prime Pairs
   Descending Wieferich Prime Pairs
   Comparing results

New Family of Binary Sequences
   Note: A generalization of Galois sequences

New Family of Polyphase Sequences
   $L^4$ norms of polynomials
   Merit Factor Comparisons
Introduction

Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Autocorrelations

Definition (Aperiodic Autocorrelation)
of a sequence of length $n$ at shift $k$, $0 \leq k < n$ is

$$c_k = \sum_{i=0}^{n-1-k} a_i \bar{a}_{i+k}$$

Definition (Periodic Autocorrelation)
of a sequence of length $n$ at shift $k$, $0 \leq k < n$ is

$$\gamma_k = \sum_{i=0}^{n-1} a_i \bar{a}_{i+k \mod (n)}$$
Barker Sequences

**Definition**

A *barker sequence* is a binary sequence \( \{a_0, a_1, ... a_{n-1}\} \) of length \( n \) such that when calculating the sequence’s aperiodic autocorrelation at shift \( k = 0 \), \( c_0 = n \) and for shift ranging from \( 1 \leq k < n \) the aperiodic autocorrelation is \( |c_k| \leq 1 \)
Example (\(\{1, 1, -1\}\))

\[
\begin{align*}
c_0 &= \sum_{i=0}^{3-1-0} a_i a_{i+0} = 1(1) + 1(1) + (-1)(-1) = 3 \\
c_1 &= \sum_{i=0}^{3-1-1} a_i a_{i+1} = 1(1) + 1(-1) = 0 \\
c_2 &= \sum_{i=0}^{3-1-2} a_i a_{i+2} = 1(-1) = -1
\end{align*}
\]

Barker Sequence!
Barker Conjecture

There exists no Barker sequence of $n > 13$

Proven for

- $n$ of odd length
- even $n = 3979201339721749133016171583224100$ or $n > 4 \times 10^{33}$

(P. Borwein & M. Mossinghoff, 2014)
Introduction

Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices

Restrictions on $n$
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences

Note: A generalization of Galois sequences

New Family of Polyphase Sequences

$L^4$ norms of polynomials
Merit Factor Comparisons
Circulant Hadamard Matrices

Definition (Hadamard Matrix)
An $n \times n$ matrix $H$ of $\pm 1$ where $HH^T = nI_n$

Definition (Circulant Matrix)
A matrix where each row after the first row is one cyclic shift to the right of the previous row.

Example (Circulant Hadamard Matrix)

\[
\begin{pmatrix}
+ & + & + & - \\
- & + & + & + \\
+ & - & + & + \\
+ & + & - & + \\
\end{pmatrix}
\]
Circulant Hadamard Matrices

Definition (Hadamard Matrix)
An $n \times n$ matrix $H$ of $\pm 1$ where $HH^T = nI_n$

Definition (Circulant Matrix)
A matrix where each row after the first row is one cyclic shift to the right of the previous row.

Example (Circulant Hadamard Matrix)
\[
\begin{pmatrix}
+ & + & + & - \\
- & + & + & + \\
+ & - & + & + \\
+ & + & - & +
\end{pmatrix}
\begin{pmatrix}
+ & - & + & + \\
+ & + & - & + \\
+ & + & + & - \\
- & + & + & +
\end{pmatrix}
= \begin{pmatrix}
4 & 0 & 0 & 0 \\
0 & 4 & 0 & 0 \\
0 & 0 & 4 & 0 \\
0 & 0 & 0 & 4
\end{pmatrix}
\]
Relationship between Barker sequences and Circulant Hadamard matrices

Definition (Circulant Hadamard Conjecture)
There exists no Circulant Hadamard Matrix with $n > 4$

Barker Sequence $\Rightarrow$ small aperiodic autocorrelations $\Rightarrow$ small periodic autocorrelations $\Rightarrow$ Circulant Hadamard Matrix
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Introduction

Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices

Restrictions on \( n \)

Ascending Wieferich Prime Pairs

Descending Wieferich Prime Pairs

Comparing results

New Family of Binary Sequences

Note: A generalization of Galois sequences

New Family of Polyphase Sequences

\( L^4 \) norms of polynomials

Merit Factor Comparisons
Restrictions

- By Definition of a Hadamard Matrix
  - Must be a multiple of 4 (or $n = 1, 2$)
- Turyn, 1965
  - Assuming $n > 2$ then
  - $n = 4m^2$
  - $m$ is odd
  - $m$ cannot be a prime power
  - More to come
\[ n = 4m^2 \]

When searching in a given bound \( M \):

\[ m = p_1 p_2 \cdots p_u \leq M \] (1)

Theorem (Turyn)

\[ p \leq (2M^2)^{\frac{1}{3}} \]
\[ n = 4M^2 \]

When searching in a given bound \( M \):

\[ p_1 \rightarrow p_2 \rightarrow \ldots \rightarrow p_1 \]
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Links

- Ascending: \( q \rightarrow p \)
  
  \[ q < p \text{ and } q^{p-1} \equiv 1 \mod p^2 \]

- Descending: \( p \rightarrow q \)
  
  \[ q < p \text{ and } p^{q-1} \equiv 1 \mod q^2 \]

- Flimsy: \( p \bowtie q \)
  
  \[ q \mid (p - 1) \]
Types of Ascending Pairs

Different Cases \( q \leftrightarrow p \)

- **Worst Case Scenario**
- Previous Search \( M = 10^{13} \)
- \( q < p \leq \min\left(\frac{M}{q}, (2M^2)^{\frac{1}{3}}\right) \)

\[
M = 5 \times 10^{14}
\]
Types of Wieferich Prime Pairs

Double Wieferich Prime Pair | Ascending and Flimsy | Strictly Ascending
Double Wieferich Prime Pair $q \Leftrightarrow p$

$$q < p \leq \min\left(\frac{M}{q}, (2M^2)^\frac{1}{3}\right)$$

**Theorem (W. Keller & J. Richstein)**

Let $p_1$ be a primitive root of the prime $q$ and define $p_2 = p_1^q \mod q^2$. Then $\{p_2^m \mod q^2 : m = 0, 1, ..., q - 2\}$ represents a complete set of incongruent solutions of $p^{q-1} \equiv 1 \pmod{q^2}$, each of which generates an infinite sequence of solutions in arithmetic progression with difference $q^2$

$$p^{q-1} \equiv 1 \mod q^2$$
Example

- \( q = 83 \)
- \( p_1 = \text{PrimitiveRoot}(q) = 2 \)
  - Primitive root generator of the multiplicative group mod \( p \)
- \( p_2 = p_1^q \mod q^2 = 1081 \)
- \( p_2^m \mod q^2, m = 0, 1, \ldots, \frac{q-3}{2} \)
- Even case: \( a = (p_2)^m + q^2 \) and \( b = q^2 - a \)
- Odd Case: \( a = (p_2)^m \) and \( b = 2q^2 - a \)
- \( a, a + 2q^2, \ldots \),
- \( m = 37 \implies a = 4871 \)
Ascending and Flimsy $q \rightarrow p$ and $p \rightsquigarrow q$

$q < p \leq \min\left(\frac{M}{3q}, (2M^2)^{\frac{1}{3}}\right)$

$q|(p - 1)$

$q^{p-1} \equiv 1(\text{mod } p^2)$
Special Ascending

Double Wieferich Prime Pairs

\[ 3 \leftrightarrow 1006003 \]
\[ 5 \leftrightarrow 1645333507 \]
\[ 83 \leftrightarrow 4871 \]
\[ 911 \leftrightarrow 318917 \]
\[ 2903 \leftrightarrow 18787 \]

Ascending and Flimsy

\[ 3 \rightarrow 1006003 \]
\[ 5 \rightarrow 20771 \]
\[ 5 \rightarrow 53471161 \]
\[ 13 \rightarrow 1747591 \]
\[ 44963 \rightarrow 5395561 \]
Strictly Ascending

$$(3 \rightarrow 11 \rightarrow 71 \rightarrow 3) \rightarrow \ldots \rightarrow (q \rightarrow p)$$

$$r \rightarrow q \rightarrow p \rightarrow r$$
Strictly Ascending

\[ q < p \leq \frac{M}{3 \times 11 \times 71 \times q} \]

\[ r \rightarrow q \rightarrow p \rightarrow r \]
Strictly Ascending

\[ q < p \leq \frac{M}{3 \cdot 11 \cdot 71 \cdot q} \]

\[ q < p \leq \frac{M}{r \cdot q} \]

\[ q < p \leq \frac{M}{q^2} \]
Strictly Ascending

\[ q < p \leq \min(\max\left(\frac{M}{3 \times 11 \times 71 \times q}, \frac{M}{r \times q}, \frac{M}{q^2}\right), (2M^2)^{\frac{1}{3}}) \]
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
1: List $A$ and List $B = \text{All primes in Ascending Pairs}$
2: while Length $B > 0$ do
3:     for $p \in B$ do
4:         for All Primes, $q$, such that $3 \leq q < p$ do
5:             if $p^{q-1} \equiv 1 \mod q^2$ then
6:                 Add $(p, q)$ to solid link list and add $q$ to $T$
7:             else if $q | (p - 1)$ then
8:                 Add $(p, q)$ to flimsy link list and add $q$ to $T$
9:             end if
10:         end for
11:     end for
12:     $B = T/A$, $A = A \cup B$, and Clear $T$
13: end while
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on $n$
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Comparing results

<table>
<thead>
<tr>
<th></th>
<th>$10^{13}$</th>
<th>$5 \times 10^{14}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>M Bound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vertices</td>
<td>643931</td>
<td>15342</td>
</tr>
<tr>
<td>Ascending</td>
<td>59837</td>
<td>6616</td>
</tr>
<tr>
<td>Descending</td>
<td>1673025</td>
<td>33935</td>
</tr>
<tr>
<td>Flimsy</td>
<td>1729116</td>
<td>33264</td>
</tr>
</tbody>
</table>
Creating Circuits

- Johnson’s Circuit Finding Algorithm and Augmenter = 501630
- F Test
  - $M = 10^{13}$ cycles 2064
  - $M = 5 \times 10^{14}$ cycles 6683
- Turyn Test
- Leung Schmidt Test Theorem 1,5,10
\( v_p(m) = \) multiplicity of \( p \) in factorization of \( m \)

\( m_q = q\)-free and squarefree part of \( m \): \( m_q = \prod_{p|m, p \neq q} p \)

\( b(p, m) = \max_{q|m, q \leq p} \{ v_p(q^{p-1} - 1) + v_p(\text{ord}_{m_q}(q)) \} \)

\( F(m) = \gcd(m^2, \prod_{p|m} p^{b(p,m)}) \)

**Theorem**

If \( n = 4m^2 \) is the order of a circulant Hadamard matrix, then \( F(m) \geq m\phi(m) \)
Turyn Test

Definition
a is semi-primitive mod b: \( a^j \equiv -1 \mod b \) for some j

Definition
r is self-conjugate mod s: For each \( p | r \), p is semi-primitive mod the p-free part of s.

Theorem
If \( n = 4m^2 \) is the order of a Circulant Hadamard Matrix, \( r | m, s | n, \)
gcd\((r, s)\) has \( k \geq 1 \) distinct prime divisors, and r is self-conjugate mod s, then \( rs \leq 2^{k-1}n \)
Turyn Test

Theorem

If \( n = 4m^2 \) is the order of a Circulant Hadamard Matrix, \( r \mid m, s \mid n, \)
gcd\((r, s)\) has \( k \geq 1 \) distinct prime divisors, and \( r \) is self-conjugate mod \( s \), then \( rs \leq 2^{k-1}n \)

\[
L_m = \{ p_1, p_2, \ldots, p_u \}
\]

\[
L_n = \{ 2, 2, p_1, p_2, \ldots, p_u, p_1, p_2, \ldots, p_u \}
\]

Let \( \alpha \in L_m \) and \( \beta \in L_n \)

Take \( \alpha \cap \beta \)

If \( rs > 2^{k-1}n \) and \( r \) self-conjugate mod \( s \) \( \Rightarrow \) throw it out
# Cycles that Fail

<table>
<thead>
<tr>
<th>Length</th>
<th>Starting Value</th>
<th>Turyn</th>
<th>LS5</th>
<th>LS10</th>
<th>LS1</th>
<th>Surviving</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>59</td>
<td>50</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>296</td>
<td>192</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>87</td>
</tr>
<tr>
<td>5</td>
<td>915</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1744</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1946</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1229</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>430</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1st New Cycle! \( m = 10010975913705 \)
Largest m value cycle found $m=499317956344211$
Given \((p, q)\), both \(p\) and \(q\) must be \(\equiv 1 \mod 4\)
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Merit Factor

- Given a sequence $A = \{a_k\}_{k=0}^{d-1}$ of length $d$, recall that the 
  aperiodic autocorrelation at shift $u$ is

$$c_u = \sum_{j=0}^{n-d-1} a_j a_{j+u}$$

**Definition**

The merit factor of $A$ is defined to be

$$MF(A) = \frac{d^2}{2 \sum_{u=0}^{d-1} |c_u|^2}$$

- Engineering Application: measures how large peak energy of a
  signal is compared to total sidelobe energy
Binary vs Polyphase

- *Binary* and *polyphase* sequences with large merit factor are useful!

- **Binary sequence**
  - Values in \{+1, −1\}
  - No known infinite family of sequences for which merit factor grows without bound

- **Polyphase sequence**
  - Values in \(\{e^{\frac{2\pi i}{N}} \cdot q \mid q \in \mathbb{Z}\}\), for some fixed \(N\)
  - Known families of sequences with unbounded (polynomial) merit factor growth
Motivation: Barker Sequences - Binary Sequences with Best Merit Factor?

- Barker sequences appear to have the largest merit factors relative to the length of the sequence.

- Sadly, no Barker sequence of length $N > 13$ is known to exist.
Merit Factor Problem

Let $A_n$ be the set of all binary sequences of length $n$.

Definition

$$F_n := \max_{A \in A_n} MF(A),$$

the maximal value of the merit factor among sequences of length $n$.

Open Question (The Merit Factor Problem)
What is $\limsup_{n \to \infty} F_n$?
Families of Binary sequences with Large Merit Factor

- Asymptotically, merit factor of these sequences is a relatively large constant:
  - Legendre: 3
  - Galois: 3
  - Rudin-Shapiro: 3
  - Rotated Legendre: 6
  - Rotated and truncated Legendre: 6.34

- Such infinite families are relatively hard to find
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on $n$
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
A generalization of Galois sequences

- Galois sequences - binary sequences based on canonical additive characters of Galois extensions of $F_2$
- We extend to other prime bases (yielding polyphase sequences) and observe similar behavior

Definition
For prime $p$ and $m \geq 2$, consider the Galois extension $F_{p^m}$ over $F_p$. The relative trace of $F_{p^m}$ over $F_p$ is

$$\text{Tr}: F_{p^m} \longrightarrow F_p$$

$$\beta \longmapsto \sum_{j=0}^{m-1} \beta^{p^j}$$
Let $\zeta = e^{\frac{2\pi i}{p}}$, and $\theta$ be a primitive element of the group $(\mathbb{F}_{p^m})^\ast$.

**Definition**

The canonical additive character of $\mathbb{F}_{p^m}$ is given by

$$
\chi : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_p \\
\text{where } c \longmapsto \zeta^{\text{Tr}c}
$$

Then the generalized Galois sequence of length $p^m$ with respect to $\theta$ is given by the coefficient sequence of the polynomial

$$
Y_{p,m,\theta}(z) = \sum_{i=0}^{p^m-2} \chi (\theta^i) z^i
$$
Conjecture

Let $y_{p,m,\theta}$ denote the generalized Galois sequence of length $p^m$ with respect to $\theta$. We conjecture that for a fixed prime $p$, we have

$$\lim_{m \to \infty} MF(y_{p,m,\theta}) = 3$$

and for a fixed exponent $m$, we have

$$\lim_{p \to \infty} MF(y_{p,m,\theta}) = 3$$
A New Family

- based on rows of certain matrices

**Definition**

A *Walsh matrix* is a square matrix of dimension $2^k$ for some integer $k \geq 1$, defined recursively via

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$H_k = \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{bmatrix} = H_1 \otimes H_{k-1}$$
Dimension $2^1$
Dimension $2^2$
Dimension $2^4$
Dimension $2^8$
Dimension $2^{10}$
- Above ordering for Walsh Matrix is natural
- Corresponds to the Hadamard Transform (without normalization), equivalent to a multidimensional discrete Fourier transform (DFT) of size $2 \times 2 \times \cdots \times 2$ $n$ times
- We use different ordering due to Bespalov, 2009
Definition

A Walsh matrix in Bespalov ordering is a square matrix of dimension $2^k$ for some integer $k \geq 1$, defined recursively via

$$V_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$V_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$

$$V_n = \begin{bmatrix} V_{n-1} & V_{n-1}P_{n-1} \\ P_{n-1}V_{n-1} & -P_{n-1}V_{n-1}P_{n-1} \end{bmatrix}$$

where $P_n$ is a $2^n \times 2^n \{0, 1\}$-matrix with 1 on the secondary diagonal.

- New family of binary sequences constructed by concatenating rows of Walsh matrices in Bespalov ordering.
Dimension $2^1$
Dimension $2^2$
Dimension $2^4$
Dimension $2^8$
Dimension $2^{10}$
Dimension $2^{12}$
Experimental Results

*Merit factors of Walsh sequences in Bespalov enumeration, length $2^{2n}$*

<table>
<thead>
<tr>
<th>n</th>
<th>MF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.00000</td>
</tr>
<tr>
<td>2</td>
<td>3.20000</td>
</tr>
<tr>
<td>3</td>
<td>3.04762</td>
</tr>
<tr>
<td>4</td>
<td>3.01176</td>
</tr>
<tr>
<td>5</td>
<td>3.00293</td>
</tr>
<tr>
<td>6</td>
<td>3.00073</td>
</tr>
<tr>
<td>7</td>
<td>3.00018</td>
</tr>
<tr>
<td>8</td>
<td>3.00005</td>
</tr>
</tbody>
</table>
Experimental Results

- Simulated annealing \((10^6\ \text{trials})\) on the matrix row order did not find any better rearrangements

Conjecture

Let \(\{B_n\}\) denote the family of sequences defined via Bespalov’s enumeration of Walsh matrices. Then

\[
\lim_{n \to \infty} MF(B_n) = 3
\]
Introduction

Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
$L^4$ norms of polynomials

- Provides other viewpoint for Merit Factor Problem
- For each binary (resp. polyphase) sequence $\{a_k\}_{k=0}^{n-1}$, can form polynomials with binary (resp. unimodular) coefficients

$$f_n = \sum_{k=0}^{n-1} a_k z^k$$

**Definition**

Let $p \geq 1$. For a polynomial $f \in \mathbb{C}[z]$, its $L^p$ norm on the complex unit circle is given by

$$\|f\|_p = \left( \frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^p \, d\theta \right)^{1/p}$$
\( L^4 \) norm vs. Merit Factor

- Let \( f \in \mathbb{C}[z] \) be of degree \( d - 1 \) with coefficient sequence \( A \).
  By Parseval’s Theorem, write
  \[
  \|f\|_2^2 = d
  \]

- Since \( \bar{z} = 1/z \) on the unit circle,
  \[
  \|f\|_4^4 = \|f(z)\overline{f(z)}\|_2^2 = \sum_{u=1-d}^{d-1} c_u z^u = d^2 + 2 \sum_{u=0}^{d-1} |c_u|^2
  \]

- Thus
  \[
  MF(A) = \frac{d^2}{2 \sum_{u=0}^{d-1} \left| c_u \right|^2} = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4}
  \]
A question due to Littlewood

**Question**

How slowly can $\|p_n\|^4_4 - \|p_n\|^2_2$ grow for a sequence of polynomials $\{p_n\}$ with unimodular coefficients and increasing degree?

**Theorem (Schmidt, 2013)**

*For the sequence $\{h_N\}$ of polynomials given by*

$$h_N(z) = \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \zeta^{jk} z^{iN+k},$$

*where $\zeta = e^{2\pi i/N}$, we have*

$$\lim_{N \to \infty} \frac{\|h_N\|^4_4 - \|h_N\|^2_2}{\|h_N\|^3_2} = \frac{4}{\pi^2}.$$
A New Family of Polynomials

Definition
For each integer \( N \geq 1 \), write \( \zeta = e^{\frac{2\pi i}{N}} \), \( \omega = e^{\frac{\pi i}{N}} \). Define a new family of polynomials \( \{ f_N \} \), where \( f_N \) is of degree \( N^2 - 1 \), given by

\[
f_N(z) = \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} x(jN+k) z^{jN+k},
\]

where

\[
x_{jN+k} = \begin{cases} 
\zeta^k (-\omega)^{j+k}, & \text{if } N \text{ is even} \\
\zeta^k (-\omega)^j (-1)^k, & \text{if } N \text{ is odd}
\end{cases}
\]
Same asymptotic behavior as that of \( \{ h_N \} \):

**Proposition**

\[
\lim_{N \to \infty} \frac{\| f_N \|_4^4 - \| f_N \|_2^4}{\| f_N \|_2^3} = \frac{4}{\pi^2}
\]
Outline of Proposition

Use Schmidt’s method for determining the asymptotic behavior of the $L^4$ norm:

- Specializing our previous formula for the $L^4$ norm,

\[
\| f_N \|_4^4 = N^4 + 2 \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} |c_{uN+v}|^2
\]
Outline of proposition

- (Long) algebraic manipulations on the second sum to obtain Lemma

\[ \| f_N \|_4^4 = \begin{cases} 
N^4 - N^2 + 8N \sum_{1 \leq v \leq \frac{N}{2}} \sum_{1 \leq k \leq v} \frac{\sin^2 \left( \frac{(2k-1)\pi}{2N} \right)}{\sin^2 \left( \frac{\pi v}{N} \right)} & \text{if } N \text{ is even} \\
N^4 + 8N \sum_{1 \leq v \leq \frac{N-1}{2}} \sum_{1 \leq k \leq v} \frac{\sin^2 \left( \frac{(2k-1)\pi}{2N} \right)}{\sin^2 \left( \frac{\pi v}{N} \right)} & \text{if } N \text{ is odd} 
\end{cases} \]
Use an analytic bound to conclude

**Lemma**

For \( N \geq 1 \), we have

\[
8N \sum_{1 \leq v \leq N} \sum_{1 \leq k \leq v} \frac{\sin^2 \left( \frac{2k-1}{2N} \pi \right)}{\sin^2 \left( \frac{\pi v}{N} \right)} = \frac{4}{\pi^2} N^3 + O(N^2)
\]

Thus

\[
\lim_{N \to \infty} \frac{\|f_N\|_4^4 - \|f_N\|_2^4}{\|f_N\|_2^3} = \frac{\|f_N\|_4^4 - N^4}{N^3} = \frac{4}{\pi^2}.
\]
Open Question

Does there exist a sequence of polynomials with unimodular coefficients whose normalized asymptotic $L^4$ norm is less than $\frac{4}{\pi^2}$?
Introduction
Circulant Hadamard Matrices

The Search for Circulant Hadamard Matrices
Restrictions on n
Ascending Wieferich Prime Pairs
Descending Wieferich Prime Pairs
Comparing results

New Family of Binary Sequences
Note: A generalization of Galois sequences

New Family of Polyphase Sequences
$L^4$ norms of polynomials
Merit Factor Comparisons
Some Other Polyphase Sequences with Large Merit Factor Growth Rate

A few length $N^2$ sequences $\{x_{jN+k}\}_{0 \leq j, k < N}$, with

$$x_{jN+k} = \exp(\pi i \phi_{j,k})$$

where for

- **P1 Sequences:** $\phi_{j,k} = -(N - 2j - 1)(jN + k)/N$
- **Corrected Px Sequences:**
  $$\phi_{j,k} = \begin{cases} 
  [(N - 1)/2 - k] [N - 2j - 1]/N & \text{if } N \text{ is even} \\
  [(N - 2)/2 - j] [N - 2k - 1]/N & \text{if } N \text{ is odd}
  \end{cases}$$
- **Frank sequences:** $\phi_{j,k} = 2jk/N$
  (coeff. sequences of Schmidt’s $\{h_N\}$ above)
Comparison with other polyphase sequences

Figure: Merit Factor of Sequences vs. Square Root of Length

- **Blue**: New, Corrected P_x
- **Orange**: Frank, P1
- **Red**: P3, P4, Golomb, Chu
Experiments on Lower Order Terms

- Numerical calculations indicate that asymptotic behaviors of new/Px sequences and Frank sequences agree for order $N^2$.
- Conjectured that difference is at order about $N^{1.1}$
Goals and Future Work

- Binary merit factor conjectures: Walsh sequences in Bespalov ordering and generalized Galois sequences
- Finding other binary sequences with large asymptotic merit factor
- Does there exist an increasing sequence of polynomials with unimodular coefficients whose normalized asymptotic $L^4$ norm is less than $\frac{4}{\pi^2}$?
- The Merit Factor Problem: does the maximal value of the merit factor among sequences of length $n$ have a limit as $n$ grows without bound?
Any Questions?
Acknowledgement

We would like to thank

- Professor Michael Mossinghoff
- ICERM and the NSF
- Brown University Center for Computation and Visualization
- TAs
- Helpful comments from Dat Nguyen and Paxton Turner
Bibliography (1)

[BCJ04] Peter Borwein, Kwok-Kwong Stephen Choi, and Jonathan Jedwab.
Binary sequences with merit factor greater than 6.34.

A new enumeration of Walsh matrices.

The discrete Chrestenson transform.
Bibliography (2)


Bibliography (3)


Bibliography (4)

Littlewood polynomials with small $L^4$ norm. 

[Joh75] Donald B. Johnson. 
Finding all the elementary circuits of a directed graph. 

The $L_4$ norm of Littlewood polynomials derived from the 
Jacobi symbol. 

Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. 
Bibliography (5)

On the equivalence between one-dimensional discrete Walsh-Hadamard and multidimensional discrete Fourier transforms.  

[LN94] Rudolf Lidl and Harald Niederreiter.  
*Introduction to finite fields and their applications.*  

[LS05] Ka Hin Leung and Bernhard Schmidt.  
The field descent method.  
Bibliography (6)


Bibliography (8)

On binary sequences. 

Character sums and difference sets. 