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

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 ($\{1, 1, -1\}$)

$$c_0 = \sum_{i=0}^{3-1-0} a_i a_{i+0} = 1(1) + 1(1) + (-1)(-1) = 3$$

$$c_1 = \sum_{i=0}^{3-1-1} a_i a_{i+1} = 1(1) + 1(-1) = 0$$

$$c_2 = \sum_{i=0}^{3-1-2} a_i a_{i+2} = 1(-1) = -1$$

Barker Sequence!

Barker Conjecture

There exists no Barker sequence of $n > 13$

Proven for

- n of odd length
- even $n = 3979201339721749133016171583224100$ or $n > 4 * 10^{33}$ (P. Borwein & M. Mossinghoff, 2014)

Circulant Hadamard Matrices

Definition (Hadamard Matrix)

An $n \times n$ matrix H of ± 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)

$$\begin{matrix} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{matrix}$$

Circulant Hadamard Matrices

Definition (Hadamard Matrix)

An $n \times n$ matrix H of ± 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)

$$\begin{pmatrix} + & + & + & - \\ - & + & + & + \\ + & - & + & + \\ + & + & - & + \end{pmatrix} \cdot \begin{pmatrix} + & - & + & + \\ + & + & - & + \\ + & + & + & - \\ - & + & + & + \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

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

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:

$$m = p_1 p_2 ... p_u \leq M \tag{1}$$

Theorem (Turyn)

$p \leq (2M^2)^{\frac{1}{3}}$

$n = 4M^2$

When searching in a given bound M:

$$p_1 \rightarrow p_2 \rightarrow \ldots \rightarrow p_1$$

Links

- Ascending: $q \longrightarrow p$

$$q < p \text{ and } \quad q^{p-1} \equiv 1 \mod p^2$$

- Descending: $p \longrightarrow q$

$$q < p \text{ and } \quad p^{q-1} \equiv 1 \mod q^2$$

- Flimsy: $p \rightsquigarrow q$

$$q | (p-1)$$

Types of Ascending Pairs

Different Cases $q \leftrightarrows p$

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

$$M = 5 * 10^{14}$$

Types of Wieferich Prime Pairs

Double Wieferich Prime Pair	Ascending and Flimsy	Strictly Ascending

Double Wieferich Prime Pair $q \leftrightarrows p$

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

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 $p^{q-1} \equiv 1 (mod\ q^2)$, 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

- $q = 83$
- $p_1 = PrimitiveRoot(q) = 2$
  - Primitive root generator of the multiplicative group mod p
- $p_2 = p_1^q \bmod q^2 = 1081$
- $p_2^m \mod q^2$, $m = 0, 1, .., \frac{q-3}{2}$
- 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, $a + 2q^2$, ... ,
- $m = 37 \Rightarrow a = 4871$

Ascending and Flimsy $q \longrightarrow p$ and $p \rightsquigarrow q$

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

$$q|(p-1)$$

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

Special Ascending

Double Wieferich Prime Pairs	**Ascending and Flimsy**
$3 \leftrightarrows 1006003$	$3 \to 1006003$
$5 \leftrightarrows 1645333507$	$5 \to 20771$
$83 \leftrightarrows 4871$	$5 \to 53471161$
$911 \leftrightarrows 318917$	$13 \to 1747591$
$2903 \leftrightarrows 18787$	$44963 \to 5395561$

Strictly Ascending

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

$$r \rightarrow q \rightarrow p \rightarrow r$$

Strictly Ascending

$$q < p \leq \frac{M}{3*11*71*q}$$

$$r \rightarrow q \rightarrow p \rightarrow r$$

Strictly Ascending

$$q < p \leq \frac{M}{3*11*71*q}$$

$$q < p \leq \frac{M}{r*q}$$

$$q < p \leq \frac{M}{q^2}$$

Strictly Ascending

$$q < p \leq min\left(max\left(\frac{M}{3*11*71*q}, \frac{M}{r*q}, \frac{M}{q^2}\right), (2M^2)^{\frac{1}{3}}\right)$$

```
List A and List B = All primes in Ascending Pairs
while Length B > 0 do
    for p ∈ B do
        for All Primes, q, such that 3 ≤ q < p do
            if p^(q−1) ≡ 1 mod q^2 then
                Add (p, q) to solid link list and add q to T
            else if q|(p − 1) then
                Add (p, q) to flimsy link list and add q to T
            end if
        end for
    end for
    B = T/A, A = A ∪ B, and Clear T
end while
```

Comparing results

M Bound	10^{13}	$5 * 10^{14}$
Vertices	643931	15342
Ascending	59837	6616
Descending	1673025	33935
Flimsy	1729116	33264

Creating Circuits

- Johnson's Circuit Finding Algorithm and Augmenter= 501630
- F Test
  - $M = 10^{13}$ cycles 2064
  - $M = 5 * 10^{14}$ cycles 6683
- Turyn Test
- Leung Schmidt Test Theorem 1,5,10

F-Test Leung and Schmidt 2005

- $v_p(m) =$ multiplicity of p in factorization of m
- $m_q =$ q-free and squarefree part of m: $m_q = \prod_{p|m, p \neq q} p$
- $b(p, m) = max_{q|m, q \leq p}\{v_p(q^{p-1} - 1) + v_p(ord_{m_q}(q))\}$
- $F(m) = gcd(m^2, \prod_{p|m} p^{b(p,m)})$

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, $r|m$, $s|n$, $gcd(r, s)$ has $k \geq 1$ distinct prime divisors, and r is self-conjugate mod s, then $rs \leq 2^{k-1}n$

$$L_m = \{p_1, p_2, ..., p_u\}$$

$$L_n = \{2, 2, p_1, p_2, ..., p_u, p_1, p_2, ..., p_u\}$$

Let $\alpha \in L_m$ and $\beta \in L_n$

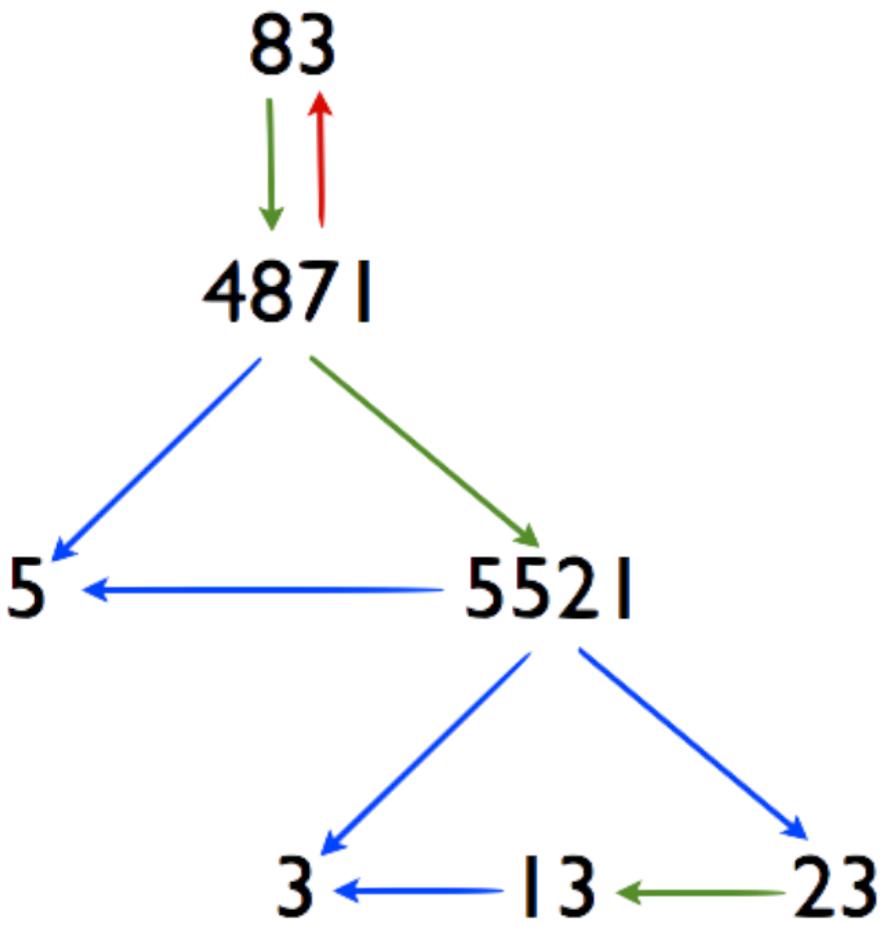
Take $\alpha \cap \beta$

If $rs > 2^{k-1}n$ and r self-conjugate mod s ->throw it out

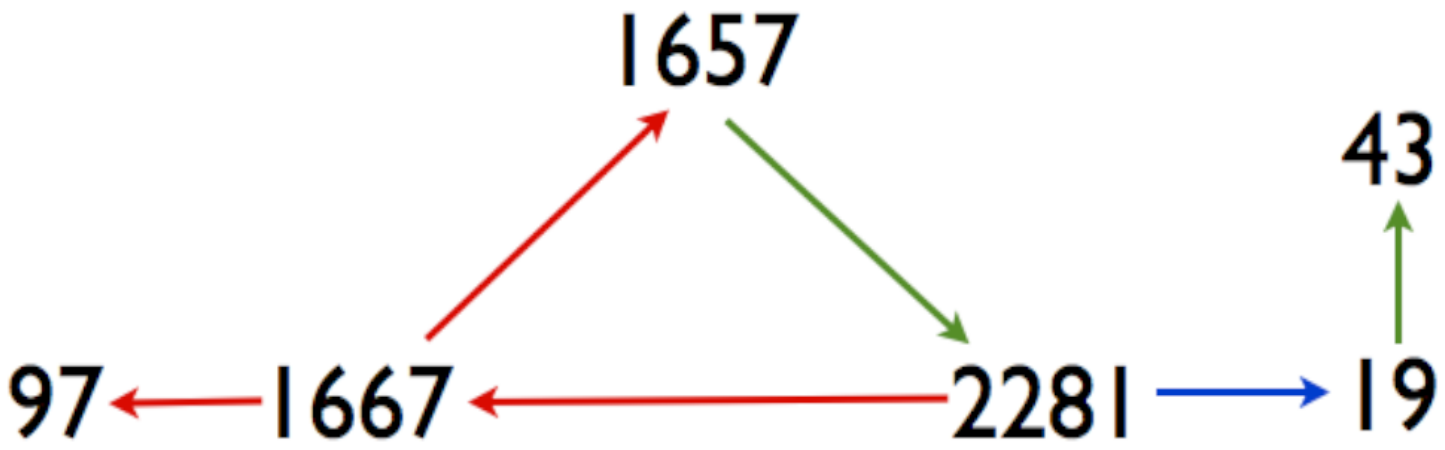
Cycles that Fail

Length	Starting Value	Turyn	LS5	LS10	LS1	Surviving
2	5	5	-	-	-	0
3	59	50	0	0	0	9
4	296	192	5	1	9	87
5	915					
6	1744					
7	1946					
8	1229					
9	430					
10	59					

1st New Cycle! m=10010975913705



Largest m value cycle found m=499317956344211



Barker

Given (p, q), both p and q must be $\equiv 1 \mod 4$

Merit Factor

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

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

Definition

The *merit factor* of A is defined to be

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

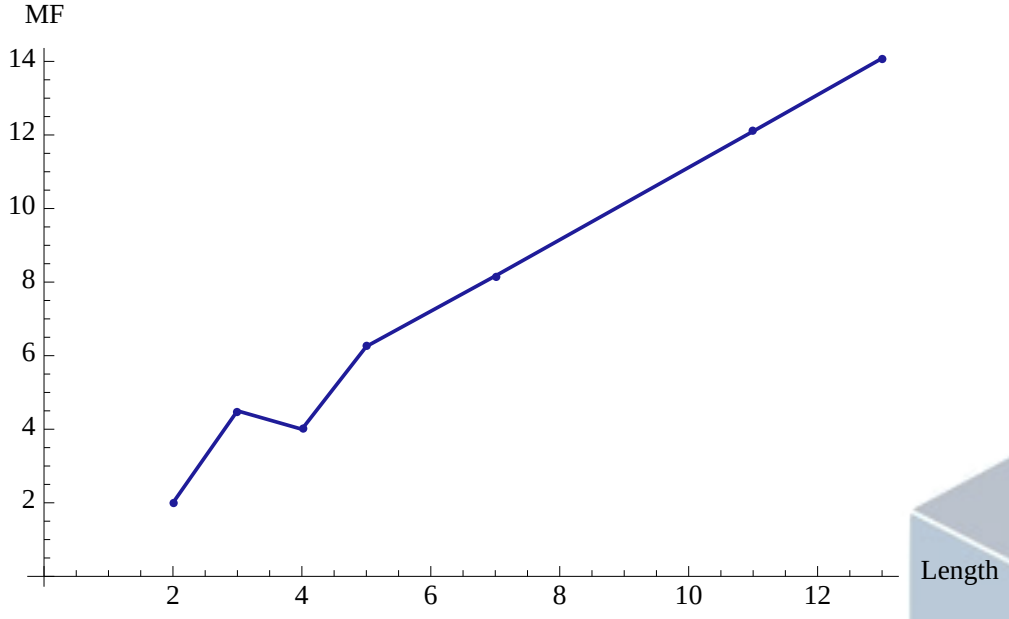
- Engineering Application: measures how large peak energy of a signal is compared to total sidelobe energy

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 $\{e^{\frac{2\pi i}{N} q} \mid q \in \mathbb{Z}\}$, 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 $\mathcal{A}_n$ be the set of all binary sequences of length n.

Definition

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

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

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 $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. The relative trace of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ is

$$\begin{aligned} \mathrm{Tr}\colon \mathbb{F}_{p^m} &\longrightarrow \mathbb{F}_p \\ \beta &\longmapsto \sum_{j=0}^{m-1} \beta^{p^j} \end{aligned}$$

Let $\zeta = e^{\frac{2\pi i}{p}}$, and θ be a primitive element of the group $(\mathbb{F}_{p^m})^*$.

Definition

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

$$\begin{aligned} \chi \colon \mathbb{F}_{p^m} &\longrightarrow \mathbb{F}_p \\ c &\longmapsto \zeta^{\mathrm{Tr}\, c} \end{aligned}$$

Then the *generalized Galois sequence of length p^m with respect to θ* is given by the coefficient sequence of the polynomial

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

Conjecture

Let $y_{p,m,\theta}$ denote the generalized Galois sequence of length p^m with respect to θ. 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

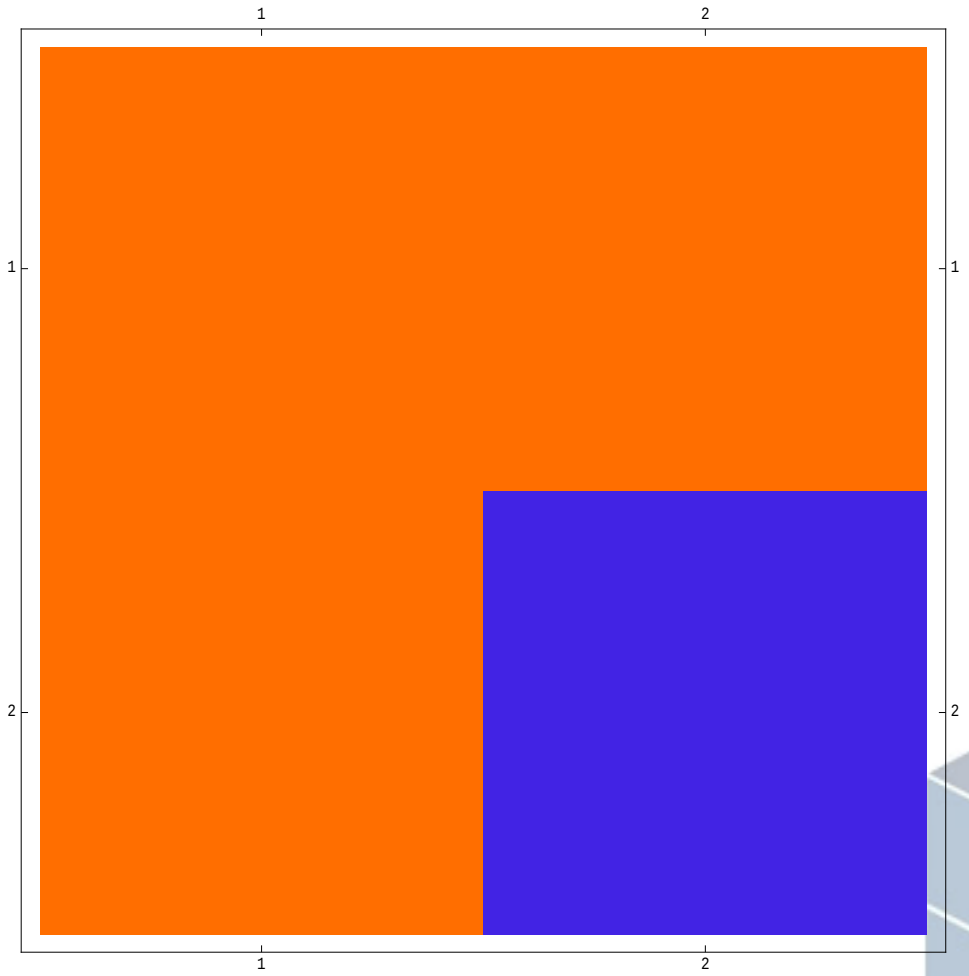
Definition

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

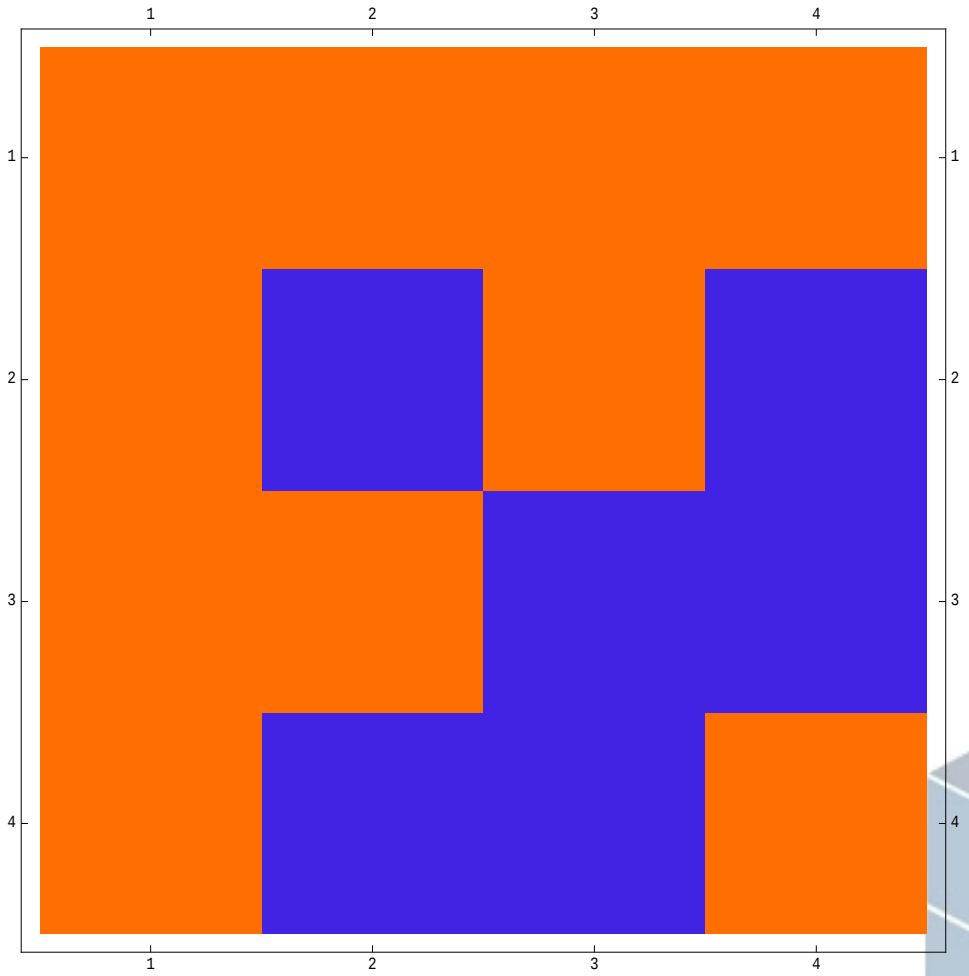
$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$H_k = \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{bmatrix} = H_1 \otimes H_{k-1}$$

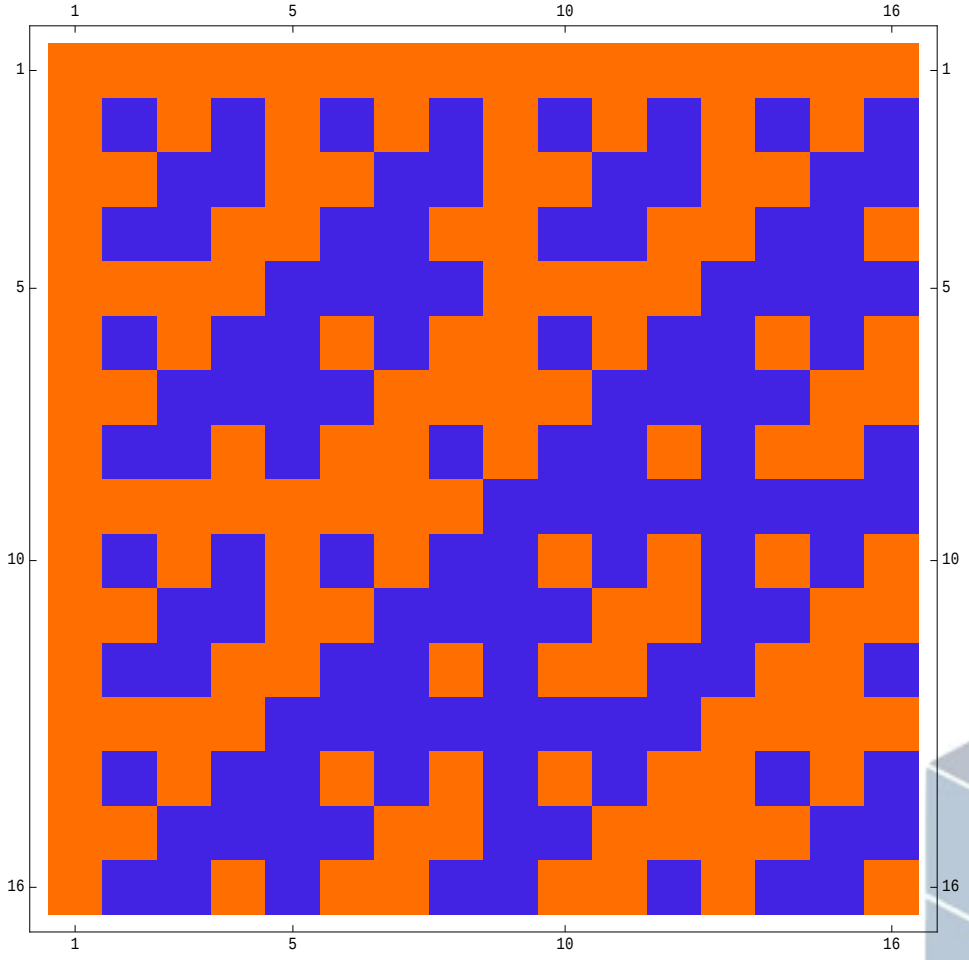
Dimension 2^1



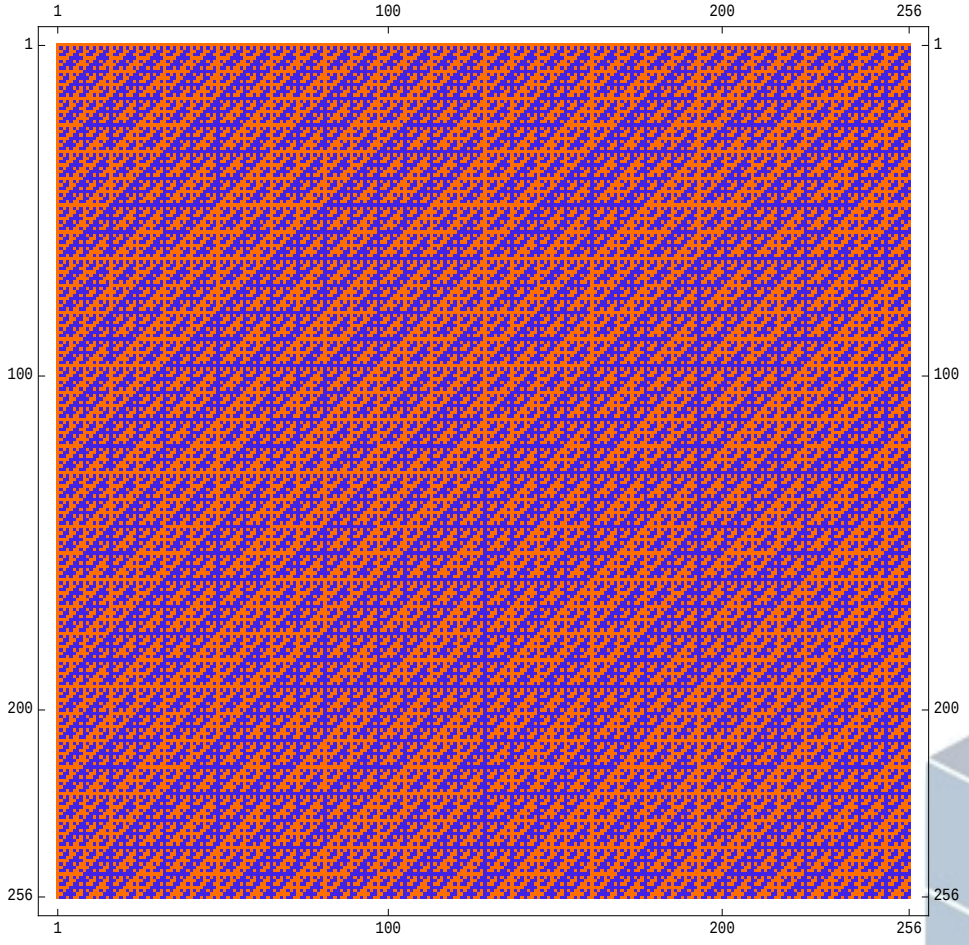
Dimension 2^2



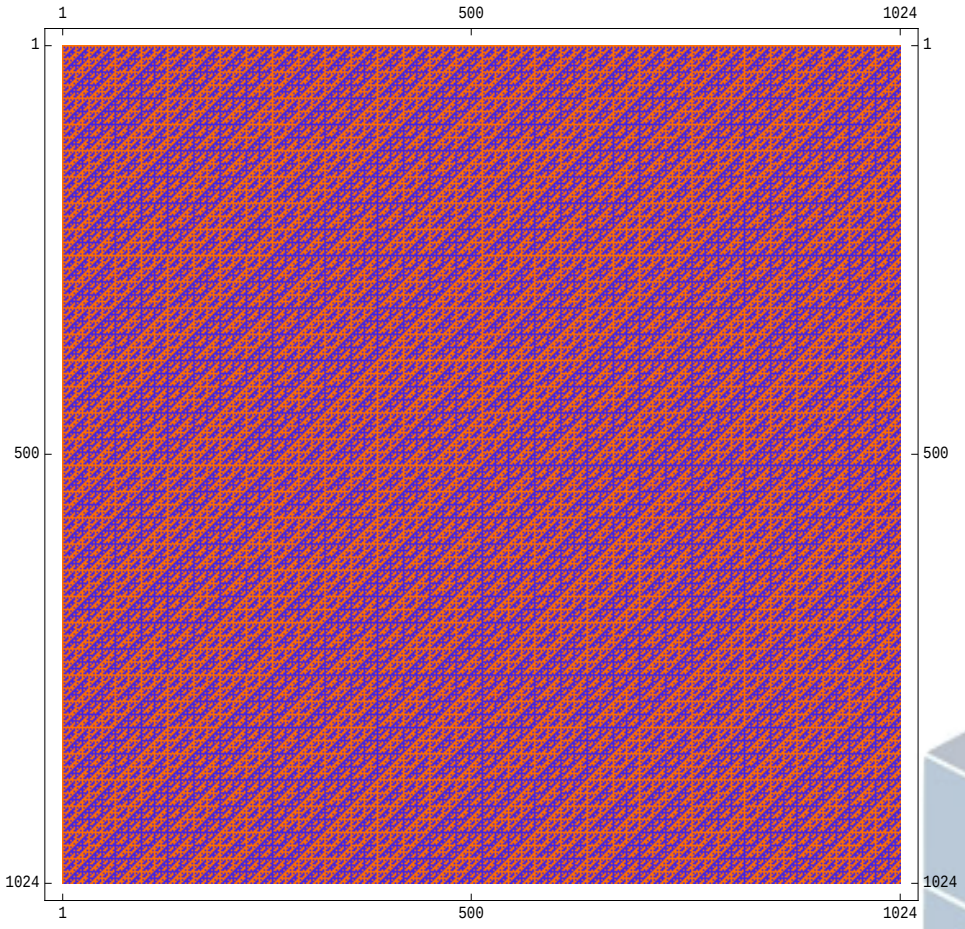
Dimension 2^4



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 $\underbrace{2 \times 2 \times \cdots \times 2}_{n \text{ times}}$
- 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

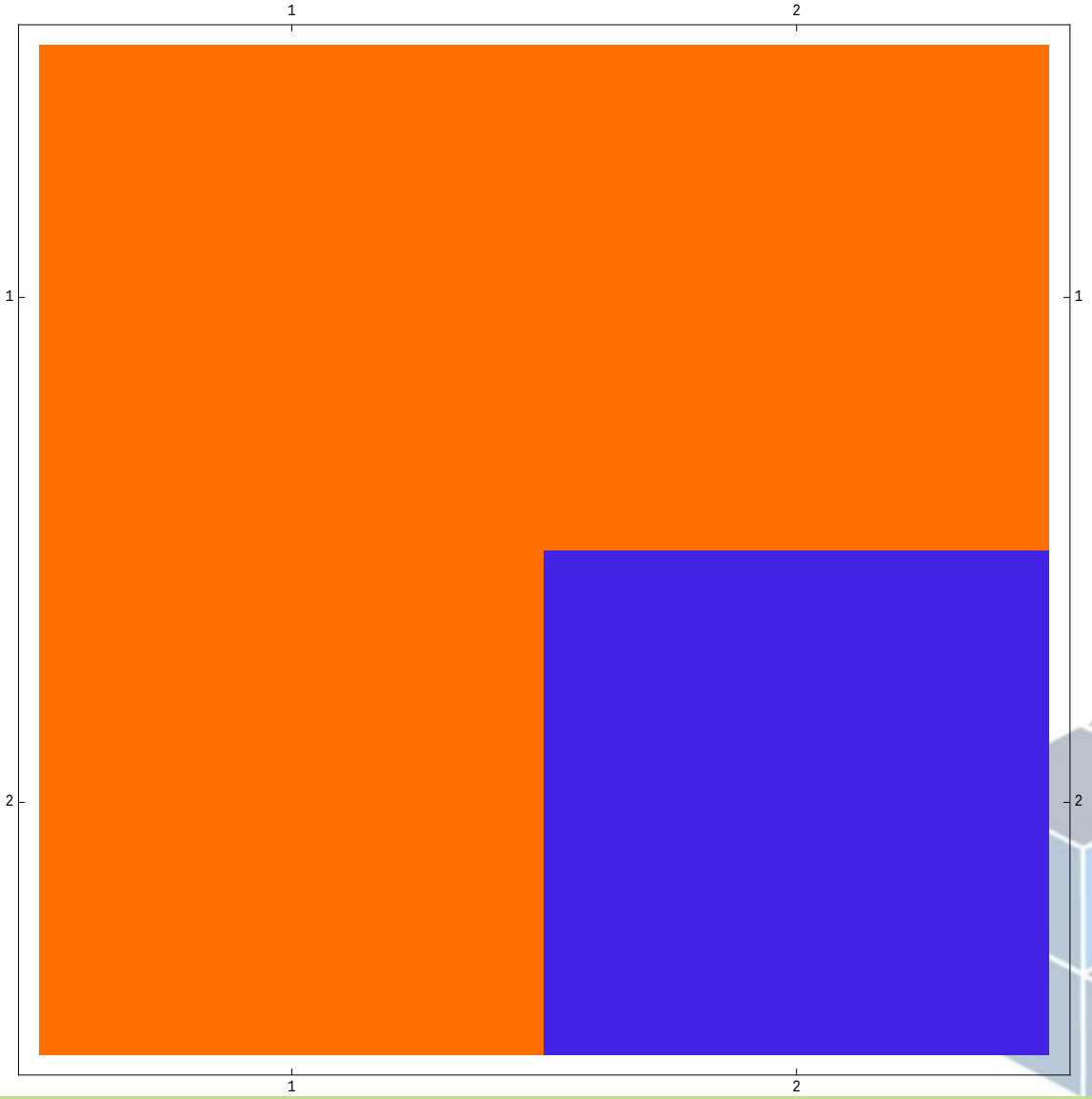
$$V_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad V_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$

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

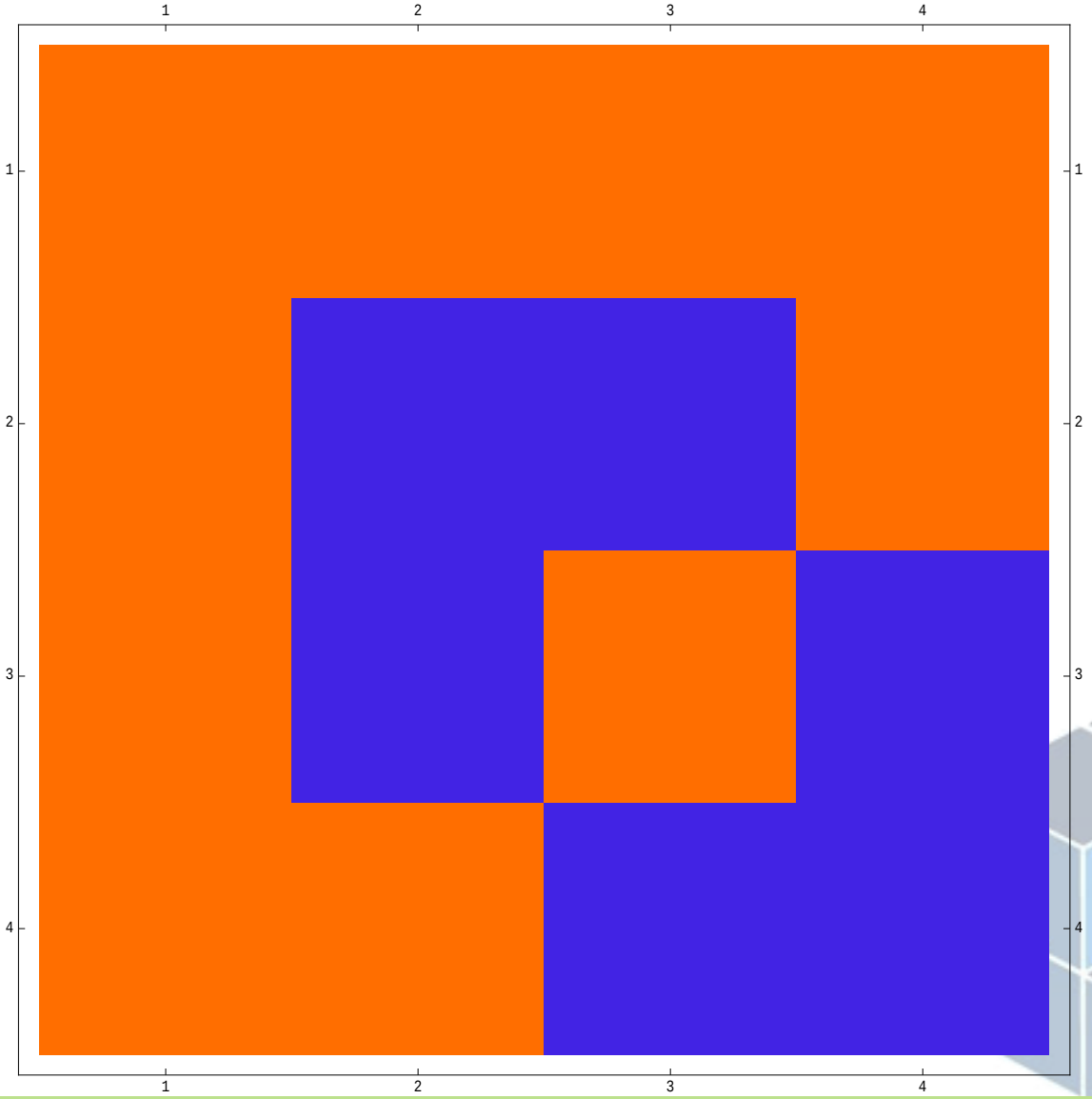
where P_n is a $2^n \times 2^n$ $\{0,1\}$-matrix with 1 on the secondary diagonal.

- New family of binary sequences constructed by concatenating rows of Walsh matrices in Bespalov ordering

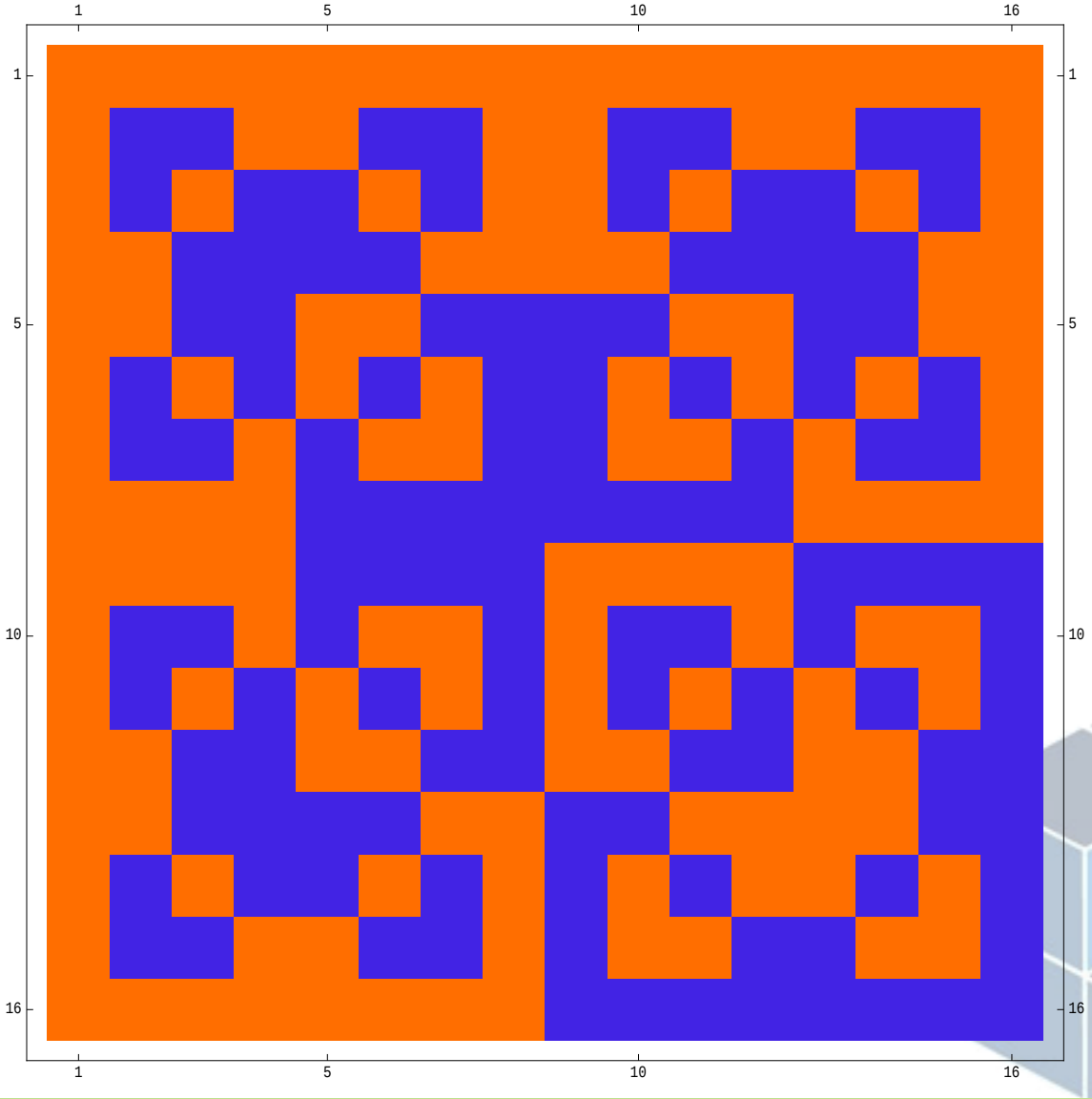
Dimension 2^1



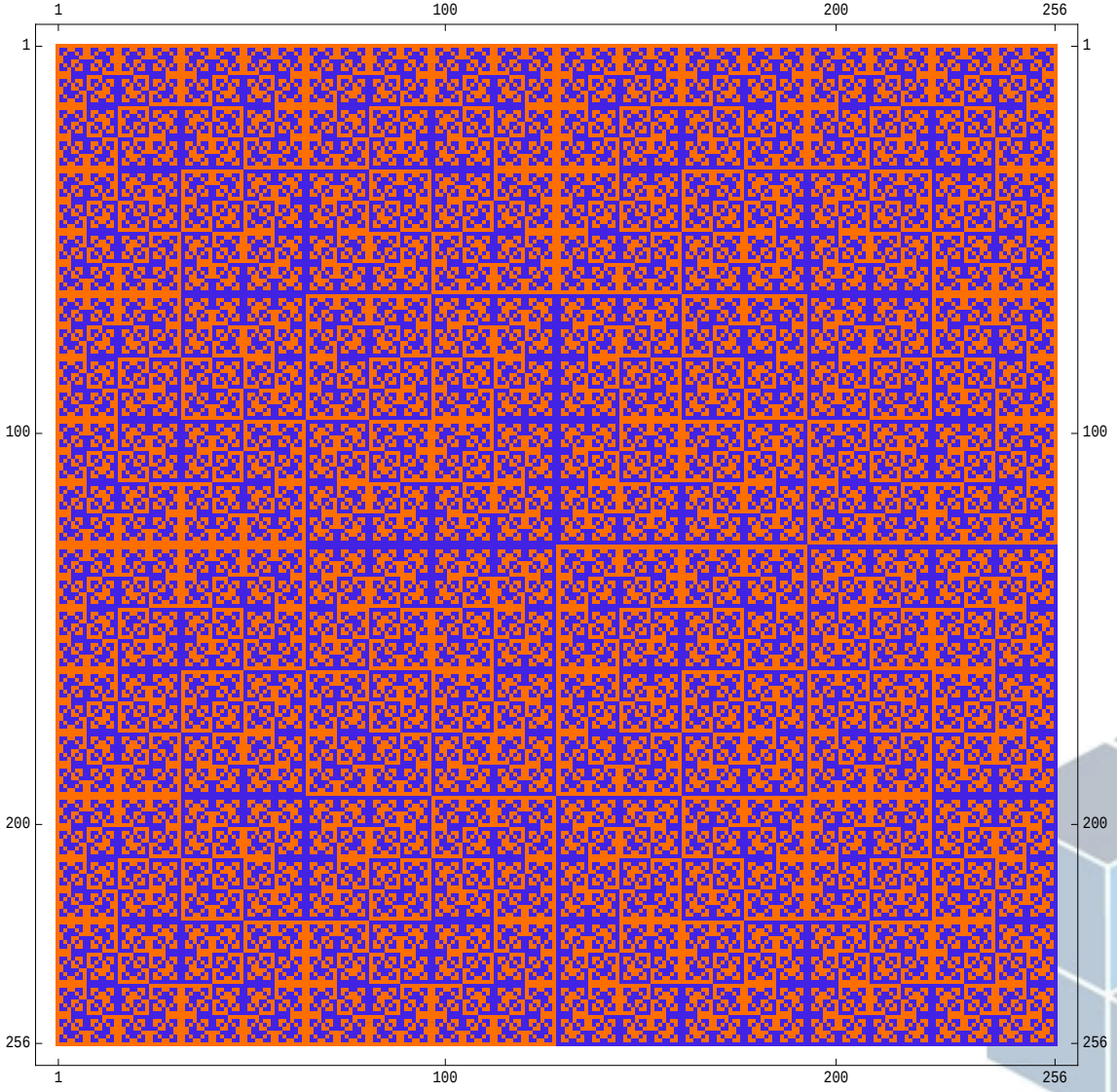
Dimension 2^2



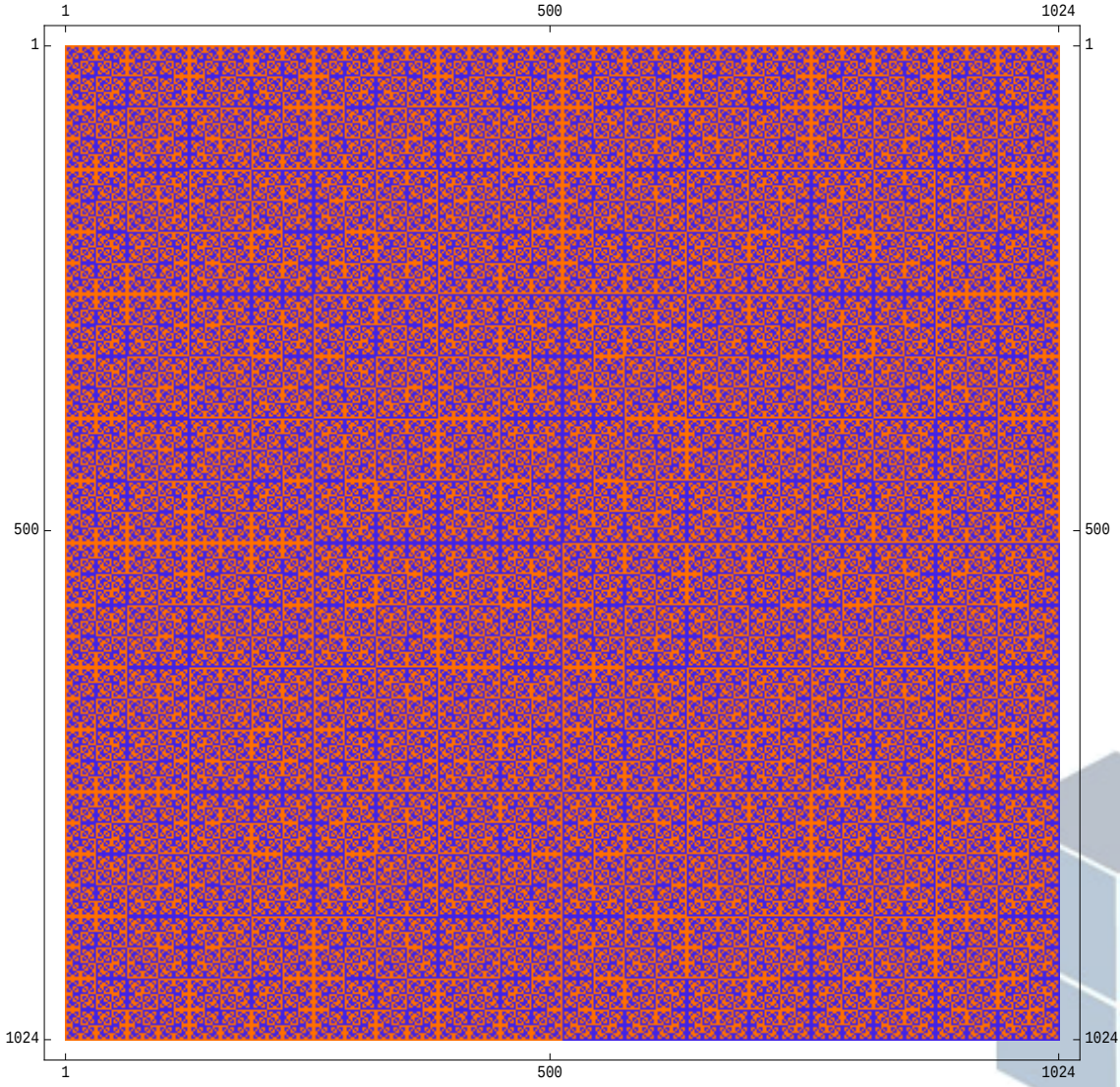
Dimension 2^4



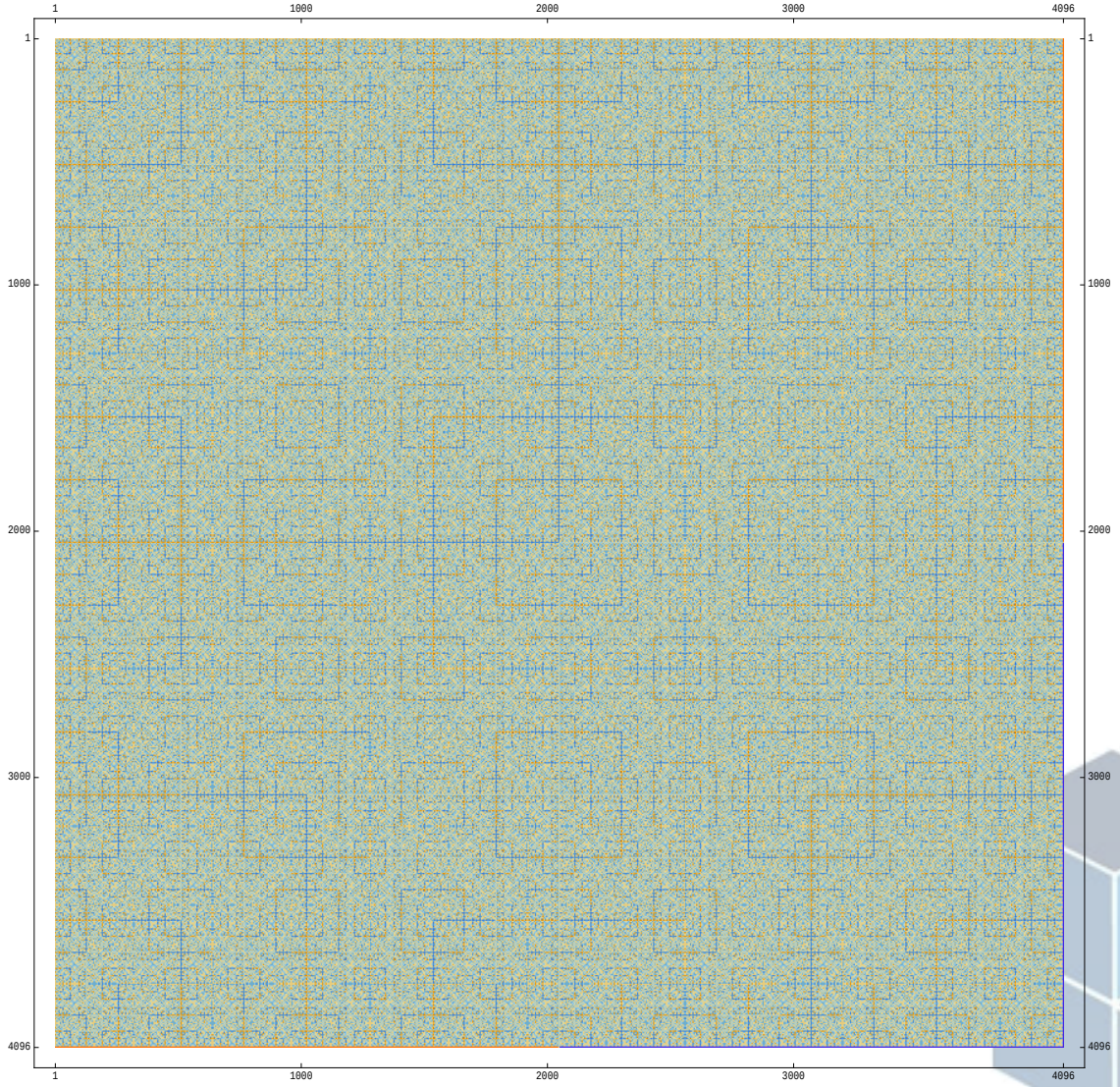
Dimension 2^8



Dimension 2^{10}



Dimension 2^{12}



Experimental Results

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

n	MF
1	4.00000
2	3.20000
3	3.04762
4	3.01176
5	3.00293
6	3.00073
7	3.00018
8	3.00005

Experimental Results

- Simulated annealing (10^6 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

$$\lim_{n\to\infty} MF(B_n) = 3$$

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

$$\|f\|_p = \left(\frac{1}{2\pi} \int_0^{2\pi} \left| f(e^{i\theta}) \right|^p d\theta \right)^{1/p}$$

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 $\overline{z} = 1/z$ 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

$$MF(A) = \frac{d^2}{2\sum_{u=0}^{d-1} |c_u|^2} = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4}$$

A question due to Littlewood

Question

How slowly can $\|p_n\|_4^4 - \|p_n\|_2^4$ 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

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

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

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

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

$$x_{jN+k} = \begin{cases} \zeta^{jk} (-\omega)^{j+k}, & \text{if } N \text{ is even} \\ \zeta^{jk} (-\omega)^{j} (-1)^{k}, & \text{if } N \text{ is odd} \end{cases}$$

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,

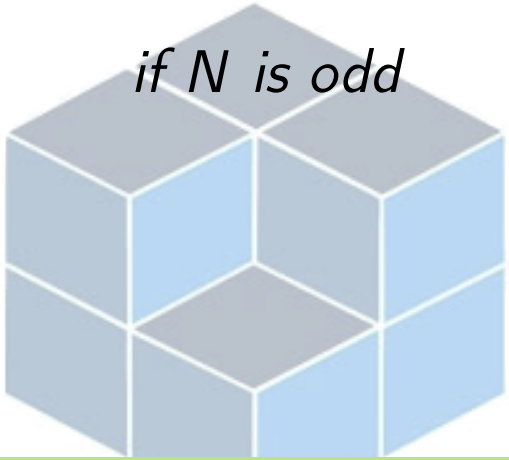
$$\|f_N\|_4^4 = N^4 + 2\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}|c_{uN+v}|^2$$

Outline of proposition

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

Lemma

$$\|f_N\|_4^4 = \begin{cases} N^4 - N^2 + 8N \displaystyle\sum_{1 \le v \le \frac{N}{2}} \sum_{1 \le k \le v} \frac{\sin^2\left(\frac{(2k-1)\pi}{2N}\right)}{\sin^2\left(\frac{\pi v}{N}\right)} & \textit{if } N \textit{ is even} \\ N^4 + 8N \displaystyle\sum_{1 \le v \le \frac{N-1}{2}} \sum_{1 \le k \le v} \frac{\sin^2\left(\frac{(2k-1)\pi}{2N}\right)}{\sin^2\left(\frac{\pi v}{N}\right)} & \textit{if } N \textit{ is odd} \end{cases}$$



- Use an analytic bound to conclude

Lemma

For $N \geq 1$, we have

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

- Thus

$$\lim_{N \to \infty} \frac{\|f_N\|_4^4 - \|f_N\|_2^4}{\|f_N\|_2^3} = \frac{\|f_N\|_4^4 - N^4}{N^3} = \frac{4}{\pi^2}. \qquad \square$$

Open Question

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

Some Other Polyphase Sequences with Large Merit Factor Growth Rate

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

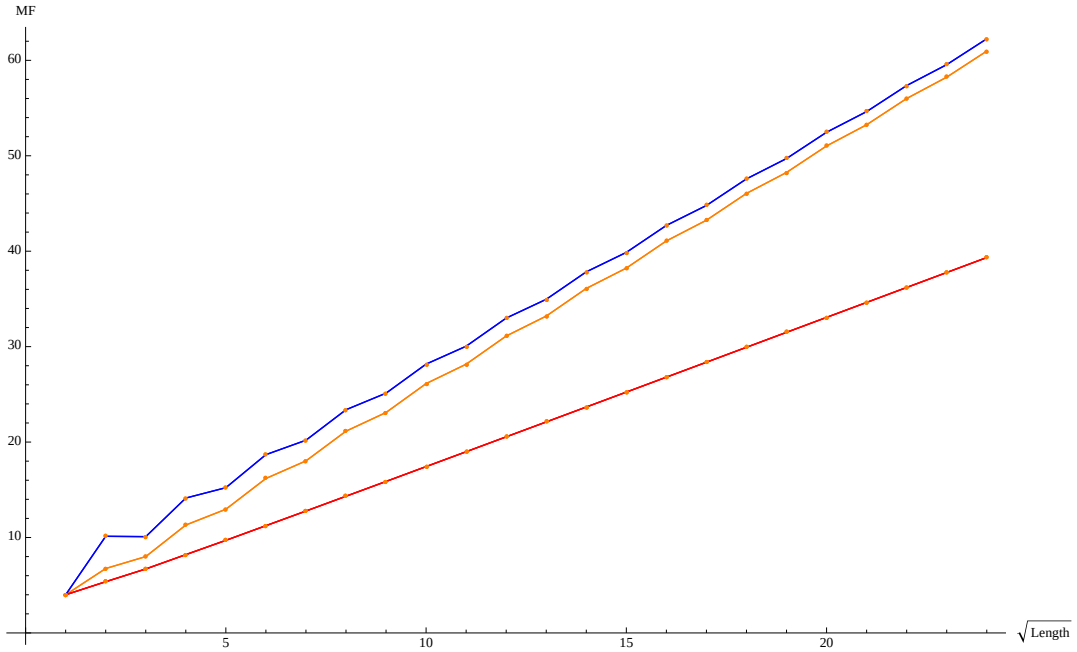


Figure : Merit Factor of Sequences vs. Square Root of Length

Blue: New, Corrected Px
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.
IEEE Trans. Inform. Theory, 50(12):3234–3249, 2004.

[Bes09] M. S. Bespalov.
A new enumeration of Walsh matrices.
Problemy Peredachi Informatsii, 45(4):43–53, 2009.

[Bes10] M. S. Bespalov.
The discrete Chrestenson transform.
Problemy Peredachi Informatsii, 46(4):91–115, 2010.

Bibliography (2)

[BM00] Peter Borwein and Michael Mossinghoff.
Rudin-Shapiro-like polynomials in L_4.
Math. Comp., 69(231):1157–1166, 2000.

[BM08] Peter Borwein and Michael J. Mossinghoff.
Barker sequences and flat polynomials.
In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 71–88. Cambridge Univ. Press, Cambridge, 2008.

[BM14] Peter Borwein and Michael J. Mossinghoff.
Wieferich pairs and Barker sequences, II.
LMS J. Comput. Math., 17(1):24–32, 2014.

Bibliography (3)

[Jed05] Jonathan Jedwab.
A survey of the merit factor problem for binary sequences.
In *Proceedings of the Third International Conference on Sequences and Their Applications*, SETA'04, pages 30–55, Berlin, Heidelberg, 2005. Springer-Verlag.

[Jed08] Jonathan Jedwab.
What can be used instead of a Barker sequence?
In *Finite fields and applications*, volume 461 of *Contemp. Math.*, pages 153–178. Amer. Math. Soc., Providence, RI, 2008.

[JKS13a] Jonathan Jedwab, Daniel J. Katz, and Kai-Uwe Schmidt.
Advances in the merit factor problem for binary sequences.
J. Combin. Theory Ser. A, 120(4):882–906, 2013.

Bibliography (4)

[JKS13b] Jonathan Jedwab, Daniel J. Katz, and Kai-Uwe Schmidt.
Littlewood polynomials with small L^4 norm.
Adv. Math., 241:127–136, 2013.

[Joh75] Donald B. Johnson.
Finding all the elementary circuits of a directed graph.
SIAM J. Comput., 4:77–84, 1975.

[JS12] Jonathan Jedwab and Kai-Uwe Schmidt.
The L_4 norm of Littlewood polynomials derived from the Jacobi symbol.
Pacific J. Math., 257(2):395–418, 2012.

[KR05] Wilfrid Keller and Jörg Richstein.
Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$.
Math. Comp., 74(250):927–936 (electronic), 2005.

Bibliography (5)

[Kun79] Henry O. Kunz.
On the equivalence between one-dimensional discrete Walsh-Hadamard and multidimensional discrete Fourier transforms.
IEEE Trans. Comput., 28(3):267–268, 1979.

[LN94] Rudolf Lidl and Harald Niederreiter.
Introduction to finite fields and their applications.
Cambridge University Press, Cambridge, first edition, 1994.

[LS05] Ka Hin Leung and Bernhard Schmidt.
The field descent method.
Des. Codes Cryptogr., 36(2):171–188, 2005.

Bibliography (6)

[LS12] Ka Hin Leung and Bernhard Schmidt.
New restrictions on possible orders of circulant Hadamard matrices.
Des. Codes Cryptogr., 64(1-2):143–151, 2012.

[Mer13] Idris Mercer.
Merit factor of Chu sequences and best merit factor of polyphase sequences.
IEEE Trans. Inform. Theory, 59(9):6083–6086, 2013.

[Mos09] Michael J. Mossinghoff.
Wieferich pairs and Barker sequences.
Des. Codes Cryptogr., 53(3):149–163, 2009.

Bibliography (7)

[MV07] Hugh L. Montgomery and Robert C. Vaughan.
Multiplicative number theory. I. Classical theory, volume 97 of *Cambridge Studies in Advanced Mathematics*.
Cambridge University Press, Cambridge, 2007.

[RK98] Predrag B. Rapajic and Rodney A. Kennedy.
Merit factor based comparison of new polyphase sequences.
IEEE Communications Letters, 2(10):269–270, 1998.

[Sch13] Kai-Uwe Schmidt.
On a problem due to Littlewood concerning polynomials with unimodular coefficients.
J. Fourier Anal. Appl., 19(3):457–466, 2013.

Bibliography (8)

[TS61] R. Turyn and J. Storer.
On binary sequences.
Proc. Amer. Math. Soc., 12:394–399, 1961.

[Tur65] Richard J. Turyn.
Character sums and difference sets.
Pacific J. Math., 15:319–346, 1965.