Exhaustive Search for the Binary Sequences of Length 2047 and 4095 with Ideal Autocorrelation

2003. 5. 24.

Seok-Yong Jin and Hong-Yeop Song

Coding and Information Theory Lab.
Yonsei University

Contents

- Introduction
- Background theory
  - Ideal autocorrelation
  - Equivalence
- Exhaustive search
  - Search methodology
  - N=2047 case
  - N=4095 case
- Conclusion: results and analysis

Introduction

- Sets of sequences in communication and cryptography
  - Random characteristic
    - Low correlation: Distinguishable from shifted version of itself and others
    - Balanced, run, span property, etc.
  - Ease of implementation
    - Linear Feedback Shift Register (LFSR) sequence
  - Security
    - Large Complexity, Long Period

- Candidates: PN-sequences

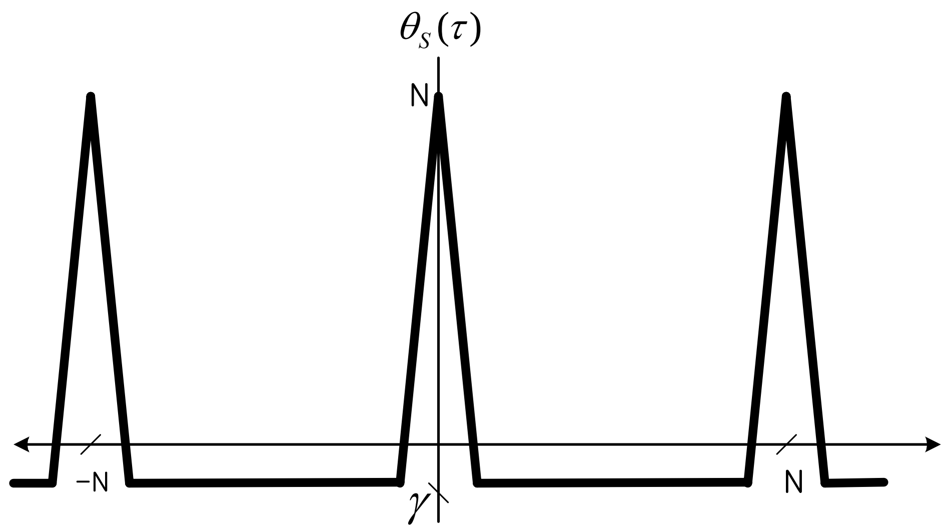
  Binary sequences with ideal autocorrelation

Ideal Autocorrelation

- Two-level autocorrelation

$$\theta_s(\tau) = \sum_{i=0}^{T-1} (-1)^{s(i)+s(i+\tau)}$$

$$= \begin{cases} T & , \tau \equiv 0 \pmod T \\ r & , else \end{cases}$$



- Out-of-phase autocorrelation as low as possible in absolute value
  - ***r = 0*** : $T=4u^2$, for $u\neq 1$, no such sequences (circulant Hadamard conjecture)
  - ***r = -1*** : called have an ideal autocorrelation property

Hadamard Sequence

- Definition

  Balanced periodic binary sequence with ideal autocorrelation (two-level autocorrelation with all out-of-phase correlation value **-1**)

- Properties
  - Length must be 4t-1 for some positive integer t.
  - Balanced: $|\ (\#\text{ of 1's}) - (\#\text{ of 0's})\ | = 1$

- Existence (Not Completely Known)
  1. $N=4t\text{-}1$ is a prime
  2. $N=p(p+2)$ is a product of "twin primes"
  3. $N=2^n\text{-}1$ for n=2, 3, 4, …

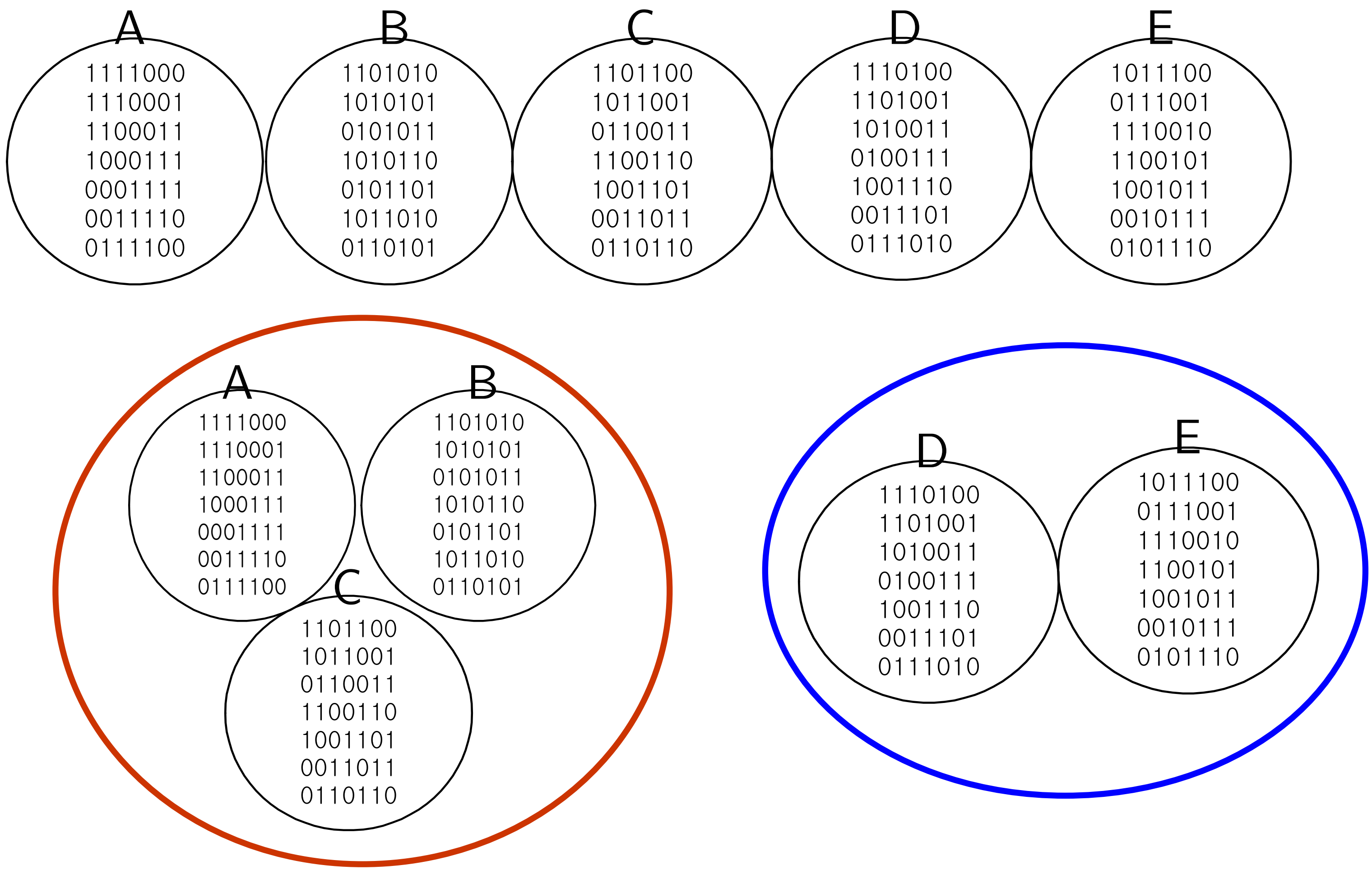
  Conjecture: These are all (verified up to 10,000 except 13 cases)

- Special interest: case 3
  - How many (truly distinct) kind?, What construction?, etc.

- S_i, $i=0, \cdots, N\text{-}1$: periodic binary sequence of length N
  - Cyclic Shifts: $U_i = S_{i+d}$ is a (cyclic) d-shifts of ***S***
  - Decimation: $R_i = S_{ti}$ with $gcd(t, N)=1$ is a t-decimation of ***S***
- *If for two same length sequence A_i and B_i, there exist t and d such that $A_i=B_{ti+d}$ for all i, then **A** and **B** are equivalent.*

- $D=\{d_1, d_2, \cdots, d_k\}$: (v,k,λ)–*cyclic difference set*
- If $tD = \{td_1, td_2, \ , td_k\} = d+D = \{d+d_1, d+d_2, \ldots, d+d_k\}$ (as a set) *for some t and d with $(t,v)=1$, then t is called a multiplier of D.*

Equivalence classes of Hadamard Sequences of Length 7



- # of (binary sequences of length 2^{11}-1 =2047) = $\mathbf{2^{2047}}$
- # of (balanced binary sequences of length 2047) ≈ $\mathbf{2^{2045}}$ $\binom{2047}{1023} \cong 2^{2045}$
- Reduction by cyclic shifts: $2^{2045}/2^{11} = 2^{2034}$
- How to reduce candidates by decimation?

  Question: Is a decimated version of Hadamard sequence also Hadamard sequence?

  Answer: Yes, due to the following.

Theorem

Any (2^n-1, 2^{n-1}-1, 2^{n-2}-1)-CHDS D has always 2 as a multiplier.

Moreover, there is unique d such that for $D'=D+d$, $2D'=D$. Then the characteristic sequence of D have the constant-on-the-coset property.

- Only to check sequences with constant-on-the-coset property: $S_i = S_{2i}$, for all i=0, …, N-1
- #(cyclotomic cosets modular 2047) = 187
  - 2^{187} candidates: still impossible!!
  - Then for what else?

Theorem (Baumert)

If a (v, k, λ)-CDS exists, then for every divisor w of v, there exists integers b_i (i=0,…,w-1) satisfying the following three equations.

$$i)\ \sum_{i=0}^{w-1} b_i = k$$

$$ii)\ \sum_{i=0}^{w-1} b_i^2 = (k-\lambda) + (\lambda v / w)$$

$$iii)\ \forall j = 1, \ldots, w-1, \quad \sum_{i=0}^{w-1} b_i b_{i-j} = \lambda v / w$$

Procedure for Exhaustive Search

1. Docompose cyclotomic cosets mod 2^{n-1}.
2. Establish & solve diophantine equations.
3. Exclude redundant solutions using decimation property.
4. Construct sequences from the solutions found. Use decimation property once again.
5. Check ideal autocorrelation.

Coset Decomposition

a_h	A_{ij}	cosets in A_{ij}	# of cosets	coset size
a_0	A_{00}	C_0	1	1
a_1	A_{01}	C_{115}	1	11
a_2	A_{02}	C_{12}	1	11
a_3	A_{03}	C_{178}	1	11
a_4	A_{04}	C_{34}	1	11
a_5	A_{05}	C_{150}	1	11
a_6	A_{06}	C_{56}	1	11
a_7	A_{07}	C_{92}	1	11
a_8	A_{08}	C_{111}	1	11
a_9	A_{10}	C_{153}	1	11
a_{10}	A_{11}	C_1 C_{20} C_{46} C_{51} C_{59} C_{76} C_{81} C_{99} C_{124} C_{146} C_{167}	11	11
a_{11}	A_{12}	C_2 C_{47} C_{49} C_{57} C_{84} C_{121} C_{134} C_{156} C_{161} C_{164} C_{185}	11	11
a_{12}	A_{13}	C_{24} C_{35} C_{60} C_{77} C_{101} C_{116} C_{118} C_{126} C_{130} C_{147} C_{173}	11	11
a_{13}	A_{14}	C_5 C_{25} C_{28} C_{79} C_{85} C_{102} C_{117} C_{132} C_{155} C_{180} C_{184}	11	11
a_{14}	A_{15}	C_{13} C_{36} C_{40} C_{42} C_{43} C_{64} C_{120} C_{122} C_{141} C_{152} C_{163}	11	11
a_{15}	A_{16}	C_7 C_{16} C_{18} C_{58} C_{65} C_{69} C_{94} C_{137} C_{166} C_{169} C_{179}	11	11
a_{16}	A_{17}	C_{14} C_{15} C_{30} C_{62} C_{67} C_{74} C_{75} C_{95} C_{145} C_{172} C_{175}	11	11
a_{17}	A_{18}	C_{21} C_{37} C_{38} C_{93} C_{97} C_{105} C_{106} C_{112} C_{131} C_{151} C_{182}	11	11
a_{18}	A_{20}	C_{44}	1	11
a_{19}	A_{21}	C_{23} C_{33} C_{45} C_{70} C_{96} C_{107} C_{154} C_{159} C_{170} C_{177} C_{181}	11	11
a_{20}	A_{22}	C_4 C_{50} C_{55} C_{63} C_{82} C_{89} C_{114} C_{133} C_{140} C_{162} C_{176}	11	11
a_{21}	A_{23}	C_3 C_9 C_{27} C_{48} C_{53} C_{72} C_{83} C_{109} C_{138} C_{160} C_{183}	11	11
a_{22}	A_{24}	C_{11} C_{39} C_{52} C_{61} C_{88} C_{108} C_{119} C_{127} C_{135} C_{143} C_{171}	11	11
a_{23}	A_{25}	C_6 C_{29} C_{34} C_{86} C_{90} C_{103} C_{110} C_{136} C_{144} C_{148} C_{186}	11	11
a_{24}	A_{26}	C_8 C_{26} C_{68} C_{73} C_{87} C_{100} C_{113} C_{123} C_{157} C_{158} C_{174}	11	11
a_{25}	A_{27}	C_{10} C_{19} C_{32} C_{66} C_{91} C_{104} C_{128} C_{129} C_{139} C_{142} C_{165}	11	11
a_{26}	A_{28}	C_{17} C_{22} C_{31} C_{41} C_{71} C_{78} C_{80} C_{98} C_{125} C_{149} C_{168}	11	11

Diophantine Equations and Decimation

- 2047 = 23·89.
- $w=23$: 4 solutions ⇒ only 2 solutions to be examined
- $w=89$: 88 solutions ⇒ only 11 solutions (not redundant)
- For one solution set $(a_0, a_1, \cdots, a_{26})$,

$$\prod_{h=0}^{h=26} \binom{N_h}{a_h} \geq 10^{25} \text{ , where } N_h = 11 \text{ for } 16\ h's$$

- Such solutions are more than $8 \cdot 10^{10}$
- Total (at least) 10^{30} candidates took more than five hundred years in pentium 2.4Ghz CPU.

Known Hadamard Sequences (length 2047)

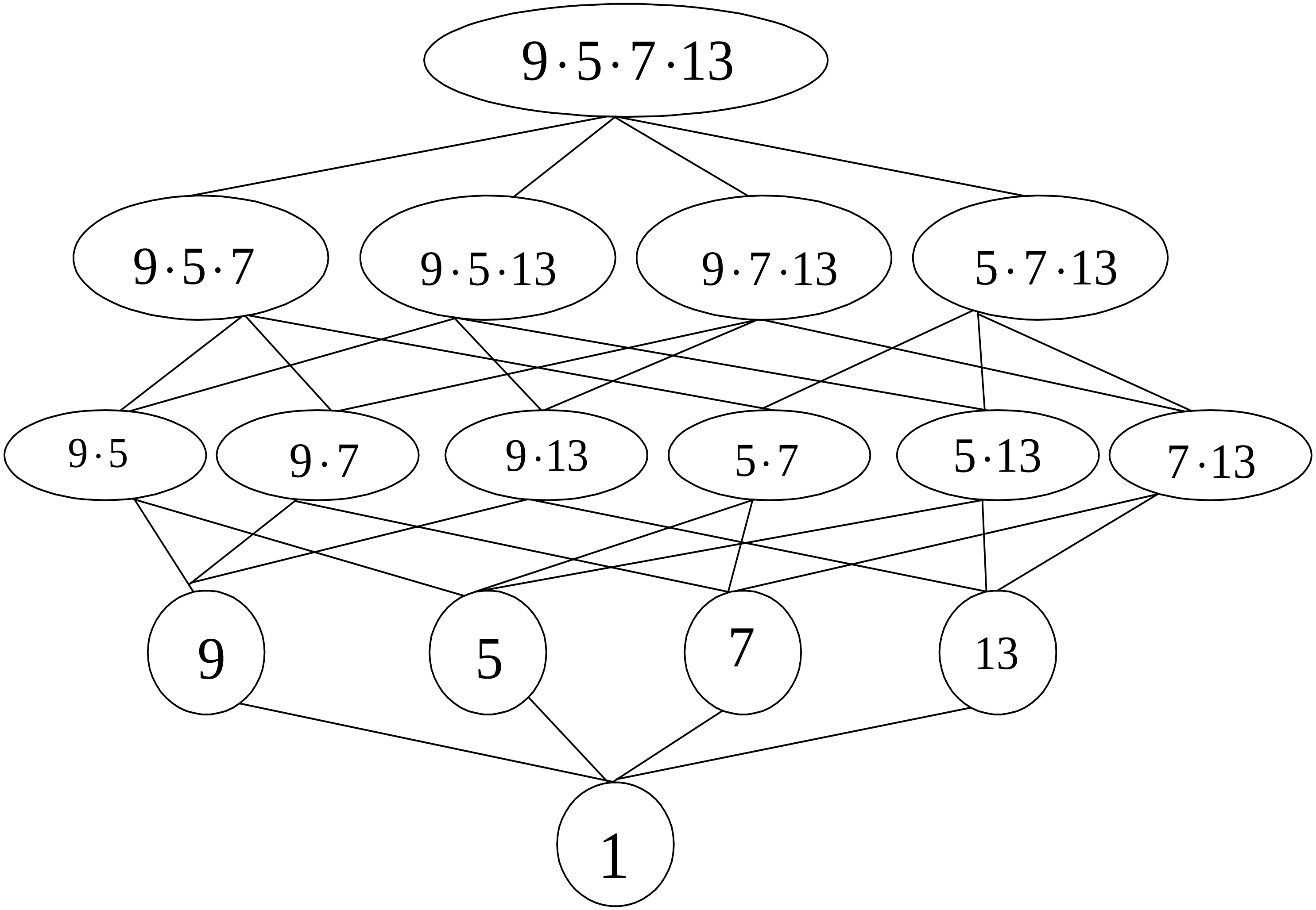
$$s(t) = Tr(\alpha^{\sum e_i t})$$

Sequence	Trace Representation
m-sequence	1
3-term sequence	1, 33, 49
5-term sequence	3, 5, 17, 73, 141
Segre hyperoval sequence	5, 25, 105, 309, 469, 83, 39, 29, 3, 19, 73, 33, 9, 17, 149
Glynn type I hyperoval	1, 5, 9, 13, 19, 37, 43, 67, 69, 137, 163, 211, 293
Glynn type II hyperoval	1, 5, 13, 17, 29, 37, 49, 61, 69, 81, 93, 101, 113, 125, 139, 147, 151, 171, 173, 183

Linear complexity of Hadamard sequences of length 2047 from monomial hyperoval in projective plane

Sequence Type	m	HS	HG_1	HG_2
Linear Span	11	165	143	231

Divisor structure of 4095



Decomposition of cyclotomic cosets mod 4095

a_i A_{ijkl}	Cosets	Class Size	Coset Size
a_0 A_{0000}	C_0	1	1
a_1 A_{0001}	C_{143}	1	12
a_2 A_{0010}	C_{220}	1	3
a_3 A_{0011}	C_{66} C_{273} C_{284}	3	12
a_4 A_{0020}	C_{341}	1	3
a_5 A_{0021}	C_{23} C_{176} C_{212}	3	12
a_6 A_{0100}	C_{275}	1	4
a_7 A_{0101}	C_{32} C_{92} C_{191} C_{251}	4	12
a_8 A_{0110}	C_{158}	1	12
a_9 A_{0111}	C_5 C_{41} C_{50} C_{100} C_{150} C_{197} C_{205} C_{227} C_{240} C_{294} C_{308} C_{332}	12	12
a_{10} A_{0120}	C_{59}	1	12
a_{11} A_{0121}	C_{14} C_{75} C_{83} C_{117} C_{127} C_{135} C_{183} C_{233} C_{268} C_{298} C_{336} C_{345}	12	12
a_{12} A_{1000}	C_{195}	1	6
a_{13} A_{1001}	C_{18} C_{85} C_{118} C_{224} C_{289} C_{317}	6	12
a_{14} A_{1010}	C_{33} C_{256} C_{334}	3	6
a_{15} A_{1011}	C_{13} C_{43} C_{48} C_{76} C_{99} C_{113} C_{125} C_{134} C_{164} C_{181} C_{193} C_{207} C_{216} C_{252} C_{260} C_{297} C_{340} C_{343}	18	12
a_{16} A_{1020}	C_{146} C_{281} C_{349}	3	6
a_{17} A_{1021}	C_3 C_{28} C_{58} C_{63} C_{71} C_{90} C_{104} C_{151} C_{159} C_{184} C_{204} C_{228} C_{238} C_{248} C_{269} C_{296} C_{304} C_{324}	18	12
a_{18} A_{1100}	C_{46} C_{239}	2	12
a_{19} A_{1101}	C_4 C_{25} C_{39} C_{60} C_{65} C_{98} C_{105} C_{131} C_{137} C_{148} C_{154} C_{166} C_{180} C_{185} C_{201} C_{219} C_{234} C_{246} C_{267} C_{272} C_{282} C_{306} C_{331} C_{337}	24	12
a_{20} A_{1110}	C_{82} C_{107} C_{119} C_{175} C_{274} C_{302}	6	12
a_{21} A_{1111}	C_1 C_6 C_{12} C_{15} C_{19} C_{22} C_{27} C_{34} C_{36} C_{40} C_{54} C_{55} C_{57} C_{61} C_{64} C_{67} C_{73} C_{74} C_{79} C_{87} C_{93} C_{95} C_{102} C_{112} C_{115} C_{122} C_{126} C_{128} C_{144} C_{145} C_{149} C_{156} C_{161} C_{162} C_{167} C_{170} C_{177} C_{182} C_{187} C_{192} C_{196} C_{199} C_{203} C_{208} C_{210} C_{213} C_{222} C_{226} C_{230} C_{237} C_{243} C_{247} C_{254} C_{265} C_{268} C_{270} C_{276} C_{277} C_{278} C_{287} C_{290} C_{295} C_{311} C_{312} C_{313} C_{318} C_{322} C_{325} C_{333} C_{335} C_{342} C_{347}	72	12
a_{22} A_{1120}	C_7 C_{70} C_{136} C_{169} C_{288} C_{326}	6	12
a_{23} A_{1121}	C_9 C_{10} C_{16} C_{21} C_{24} C_{30} C_{31} C_{37} C_{42} C_{45} C_{49} C_{51} C_{52} C_{68} C_{77} C_{81} C_{84} C_{88} C_{91} C_{96} C_{101} C_{108} C_{109} C_{110} C_{116} C_{121} C_{129} C_{133} C_{139} C_{141} C_{142} C_{153} C_{157} C_{165} C_{172} C_{173} C_{178} C_{189} C_{190} C_{198} C_{200} C_{206} C_{211} C_{215} C_{218} C_{221} C_{229} C_{232} C_{236} C_{241} C_{245} C_{250} C_{255} C_{258} C_{261} C_{262} C_{263} C_{279} C_{283} C_{285} C_{293} C_{300} C_{301} C_{309} C_{315} C_{316} C_{319} C_{327} C_{328} C_{339} C_{344} C_{350}	72	12
a_{24} A_{2000}	C_{321}	1	2
a_{25} A_{2001}	C_{53} C_{264}	2	12
a_{26} A_{2010}	C_{307}	1	6
a_{27} A_{2011}	C_8 C_{80} C_{155} C_{168} C_{188} C_{314}	6	12
a_{28} A_{2020}	C_{94}	1	6
a_{29} A_{2021}	C_{38} C_{123} C_{130} C_{231} C_{292} C_{330}	6	12
a_{30} A_{2100}	C_{124} C_{346}	2	4
a_{31} A_{2101}	C_{11} C_{72} C_{111} C_{160} C_{174} C_{286} C_{310} C_{329}	8	12
a_{32} A_{2110}	C_{20} C_{186}	2	12
a_{33} A_{2111}	C_{26} C_{29} C_{47} C_{62} C_{69} C_{86} C_{89} C_{106} C_{120} C_{132} C_{138} C_{140} C_{202} C_{214} C_{225} C_{235} C_{244} C_{249} C_{259} C_{291} C_{299} C_{320} C_{338} C_{348}	24	12
a_{34} A_{2120}	C_{217} C_{242}	2	12
a_{35} A_{2121}	C_2 C_{17} C_{35} C_{44} C_{56} C_{78} C_{97} C_{103} C_{114} C_{147} C_{152} C_{163} C_{171} C_{179} C_{194} C_{209} C_{223} C_{253} C_{257} C_{271} C_{280} C_{303} C_{305} C_{323}	24	12

(4097, 2045, 1023)-CASE (3)

- Cyclotomic cosets mod 4095: total 351 cosets

coset size	1	2	3	4	6	12
# of cosets	1	1	2	2	5	340

- Classes of cyclotomic cosets mod 4095: 36 classes

# of cosets in class	1	2	3	4	6	8	12	18	24	72
# of such classes	11	5	4	1	5	1	2	2	3	2

- For only one solution set $(a_0, a_1, , a_{36})$, approximately

$$\binom{3}{a_{i_1}}^5 \cdot \binom{4}{a_{i_2}}^4 \cdot \binom{5}{a_{i_3}} \cdot \binom{7}{a_{i_4}} \cdot \binom{9}{a_{i_5}}^2 \cdot \binom{13}{a_{i_6}}^2 \cdot \binom{19}{a_{i_6}}^2 \cdot \binom{25}{a_{i_7}}^3 \cdot \binom{72}{a_{i_8}}^2$$

number of choices of choosing candidates, which is greater than total number of possibilities for 2^{11}-1 case

Summary

- Exhaustive search for (*2047, 1023, 511*)-CHDS
  - Since *2047* is a product of only two divisors (*23* and *89*), and *11* is a prime,
  - Previous search methodology does NOT work efficiently.

- Partial Search
  - No more inequivalent Hadamard sequence of length 2047 was found.

- Exhaustive Search for (*4095, 2047, 1023*)-CHDS
  - Actually, the final case of the current exhaustive method may work.
  - Still trying