Paper Schedule of SSC'07

- **Just approved (during the conference) – LNCS**
- Important Dates:
  - **July 16 (Mon): Initial Submission**

    ssc07@calliope.uwaterloo.ca
  - Aug 28 (Sat): Review done
  - **Sept 22 (Sat): Final submission**

    ssc07@calliope.uwaterloo.ca
  - Before Christmas of 2007 (hopefully):

    Book ready for distribution

Post-doc Position available

- With **me** at Yonsei University, Seoul, Korea
- Reasonable amount of salary
- Initial contract of 1-year
  - renewal possible up to 5 more years, if you like me (^.^)
- Requirement: AT LEAST ONE GOOD PAPER per half-year
- Good chance to experience DYNAMIC KOREA

Faculty position available

Foreigner is preferred……

Source of my travel money (sorry)

- School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea
- Initial contract for either 1-year or 2-year period
- **Tenure-track or non-tenure-track**
- Reasonable amount of salary
- Good chance to experience DYNAMIC KOREA


THESE SEQUENCES USED?
A SHIFT REGISTER (OF DEGREE n) IS A "DISCRETE DELAY LINE" (WITH n "STAGES", OR BINARY STORAGE POSITIONS) WHERE AT EACH TICK OF A MASTER CLOCK, THE CONTENTS OF EACH STAGE IS SHIFTED TO THE NEXT STAGE ON THE LINE.
IF NOTHING IS COMING INTO THE SHIFT REGISTER, IT WILL BE "EMPTY" (ALL 0'S) AFTER n CLOCK TICKS.
ee-festival

Professor Golomb, Happy Birthday!

Existence of Modular Sonar Sequences of Twin-Prime Length

2007. 6.

Sung-Jun Yoon and Hong-Yeop Song

YONSEI UNIVERSITY
Coding and Information Theory Laboratory

Golomb's conjecture

- Existence of balanced binary sequences of period v with ideal two-level autocorrelation
- **(Conjecture)** Period v must be one of the following 3 types.
  - $v = 2^n - 1$ for some positive integer n
  - v = prime p of type $4k+3$
  - v = product of twin-prime $p(p+2)$
- Unknown cases of v up to 10^4 : v = **3439**, 4355, 8591, 8835, 9135, 9215, and 9423.
- For each of the above three types of length v in the conjecture, at least one simple construction is known.

Gong's construction for families of binary sequences

- Parameter = $(v^2, v, 2v+3)$

  period — number of sequences — max correlation

- Parts:
  - two binary sequences of period v with the ideal two-level autocorrelation
  - **"shift sequence"** $\underline{\mathbf{e}}$ of length v defined over Z_v
- Assembly:
  - interleaved structure

"Shift sequence"

- The "shift sequence" $\underline{\mathbf{e}} = (e_0,\ e_1,\ \cdots,\ e_{v-1})$ over Z_v must satisfy the following:

$$\left|\{e_j - e_{j+s} \mid 0 \le j < v - s\}\right| = v - s \quad \text{for all} \quad 1 \le s < v.$$

- Same as the requirements for **modular sonar sequence of length *v* mod *v***
- Two "shift sequences" in her construction are in fact the same as the following two modular sonar sequences constructed earlier:
  - Games for the case $v = 2^n - 1$ or $p^n - 1$
  - Exponential-Welch construction for the case $v = p$ of type $4k+3$

modular sonar sequence (length 15, mod 15)

e	1	3	1	7	11	3	14	15	8	8	13	7	4	14	2
15								●							
14							●							●	
13											●				
12															
11					●										
10															
9															
8									●	●					
7				●								●			
6															
5															
4													●		
3		●				●									
2															●
1	●		●												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Checks !

1 3 1 7 11 3 14 15 8 8 13 7 4 14 2

13 2 9 11 8 4 14 7 0 10 6 3 5 12

0 11 5 4 12 3 6 7 10 1 9 8 2

9 7 13 8 11 10 6 2 1 4 14 5

5 0 2 7 3 10 1 8 4 9 11

13 4 1 14 3 5 7 11 9 6

2 3 8 14 13 11 10 1 6

1 10 8 9 4 14 0 13

8 10 3 0 7 4 12

8 5 9 3 12 1

3 11 12 3 9

9 14 2 5

12 6 14

2 1

14

Real Motivation

binary sequences of period v with ideal two-level autocorrelation	$v \times v$ Modular sonar sequences (="shift sequences" $\underline{\mathbf{e}}$)
$v = p$	$v = p$
$v = 2^n - 1$	$v = 2^n - 1$
$v = p(p+2)$	**???**

ATTACK (?)

- Computer search
- Algebraic constructions
- Ad-hoc approach

$v = 3 \times 5 = 15$ (result summary)

- There are 9000 modular sonar sequences in total.
- There are 5 inequivalent classes in the sense of the transformation (multiplication/shearing/translation) given by

$$g(i) = uf(i) + si + a \pmod{m}$$

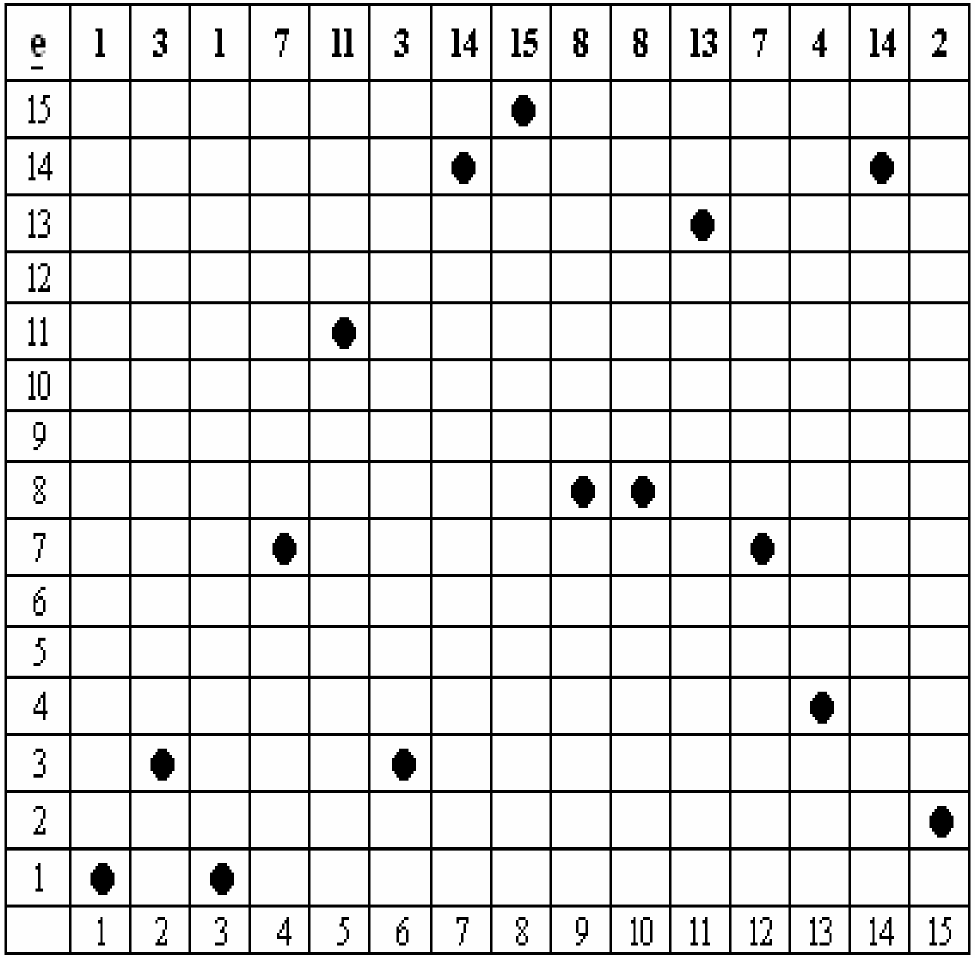
- Each class contains $8 \times 15 \times 15 = 1800$ equivalent sequences.

Representatives

- Class 1 : (1,3,1,7,11,3,14,15,8,8,13,7,4,14,2)
- Class 2 : (1,1,4,1,9,7,11,1,8,2,12,13,4,6,2)
- Class 3 : (1,1,2,14,2,13,4,9,13,12,4,2,11,6,8)
- Class 4 : (1,1,4,9,4,11,10,8,5,9,10,1,9,5,7)
- Class 5 : (1,6,12,13,10,14,7,9,7,14,10,13,12,6,1)

Palindrome !!!

Representative of Class 1



Array form of 15 x 15 Modular Sonar sequence in Class 1

1 3 1 7 11 3 14 15 8 8 13 7 4 14 2
13 2 9 11 8 4 14 7 0 10 6 3 5 12
0 11 5 4 12 3 6 7 10 1 9 8 2
9 7 13 8 11 10 6 2 1 4 14 5
5 0 2 7 3 10 1 8 4 9 11
13 4 1 14 3 5 7 11 9 6
2 3 8 14 13 11 10 1 6
1 10 8 9 4 14 0 13
8 10 3 0 7 4 12
8 5 9 3 12 1
3 11 12 3 9
9 14 2 5
12 6 14
2 1
14

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 1

Representative of Class 2

e	1	1	4	1	9	7	11	1	8	2	12	13	4	6	2
15															
14															
13												●			
12											●				
11							●								
10															
9					●										
8									●						
7						●									
6														●	
5															
4			●										●		
3															
2										●					●
1	●	●		●				●							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Array form of 15 x 15 Modular Sonar sequence in Class 2

1 1 4 1 9 7 11 1 8 2 12 13 4 6 2
0 12 3 7 2 11 10 8 6 5 14 9 13 4
12 0 10 9 13 6 3 14 11 4 8 7 2
0 7 12 5 8 14 9 5 10 13 6 11
7 9 8 0 1 5 14 3 4 11 10
9 5 3 8 7 10 14 12 2 0
5 0 11 14 12 9 7 10 6
0 8 2 4 11 3 5 14
8 14 7 3 5 1 9
14 4 6 12 3 5
4 3 0 10 7
3 12 13 14
12 10 2
10 14
14

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 2

Representative of Class 3

e	1	1	2	14	2	13	4	9	13	12	4	2	11	6	8
15															
14				●											
13						●			●						
12										●					
11													●		
10															
9								●							
8															●
7															
6														●	
5															
4							●				●				
3															
2		●			●							●			
1	●		●												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Array form of 15 x 15 Modular Sonar sequence in Class 3

1 1 2 14 2 13 4 9 13 12 4 2 11 6 8

0 14 3 12 4 9 10 11 1 8 2 6 5 13

14 2 0 1 13 4 6 12 9 10 8 11 3

2 14 4 10 8 0 7 5 11 1 13 9

14 3 13 5 4 1 0 7 2 6 11

3 12 8 1 5 9 2 13 7 4

12 7 4 2 13 11 8 3 5

7 3 5 10 0 2 13 1

3 4 13 12 6 7 11

4 12 0 3 11 5

12 14 6 8 9

14 5 11 6

5 10 9

10 8

8

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 3

Representative of Class 4

e	1	1	4	9	4	11	10	8	5	9	10	1	9	5	7
15															
14															
13															
12															
11						●									
10							●				●				
9				●						●			●		
8								●							
7															●
6															
5									●					●	
4			●		●										
3															
2															
1	●	●										●			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Array form of 15 x 15 Modular Sonar sequence in Class 4

1 1 4 9 4 11 10 8 5 9 10 1 9 5 7

0 12 10 5 8 1 2 3 11 14 9 7 4 13

12 7 0 13 9 3 5 14 10 8 1 11 2

7 12 8 14 11 6 1 13 4 0 5 9

12 5 9 1 14 2 0 7 11 4 3

5 6 11 4 10 1 9 14 0 2

6 8 14 0 9 10 1 3 13

8 11 10 14 3 2 5 1

11 7 9 8 10 6 3

7 6 3 0 14 4

6 0 10 5 12

0 7 14 2

7 11 12

11 9

9

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 4

Representative of Class 5

e	1	6	12	13	10	14	7	9	7	14	10	13	12	6	1
15															
14						●				●					
13				●								●			
12			●										●		
11															
10					●						●				
9								●							
8															
7							●		●						
6		●												●	
5															
4															
3															
2															
1	●														●
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Array form of 15 x 15 Modular Sonar sequence in Class 5

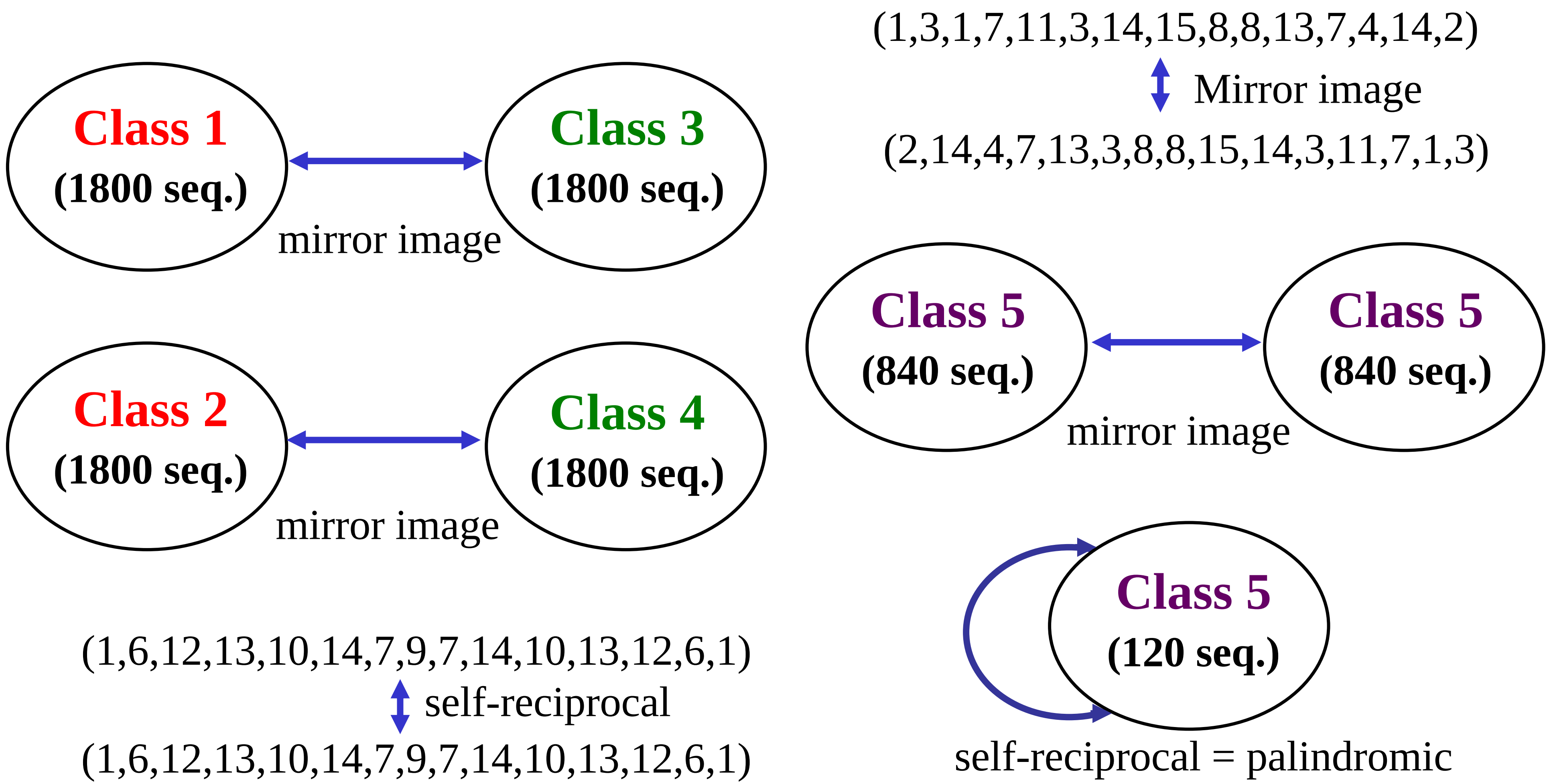
1 6 12 13 10 14 7 9 7 14 10 13 12 6 1
10 9 14 3 11 7 13 2 8 4 12 1 6 5
4 8 2 14 3 5 0 10 12 1 13 7 11
3 11 13 6 1 7 8 14 9 2 4 12
6 7 5 4 3 0 12 11 10 8 9
2 14 3 6 11 4 9 12 1 13
9 12 5 14 0 1 10 3 6
7 14 13 3 12 2 1 8
9 7 2 0 13 8 6
2 11 14 1 4 13
6 8 0 7 9
3 9 6 12
4 0 11
10 5
0

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 5

Class 5 is new!!

- The size 15 modulo 15 example can only be covered by the construction given by Games.
- The sequences in Classes 1 and 2 cover all the possible 15×15 modular sonar sequences constructed by Games.
- Class 3 (and 4) is obtained from Class 1 (and 2) by taking the mirror image of each other.

Some Relation



Some property of Class 5

- 120 sequences in Class 5 are "palindrome", that is,

$$f(i) = f(v-i),\ 0 \le i \le v \tag{1}$$

- For any palindromic sequence in Class 5, the first 8 symbols satisfy:

$$\left|\{d(s,j) = [e_j - e_{j+s}] \ne 0 \mid 0 \le j < 8-s\}\right| = 8-s \qquad 1 \le s < 8 \tag{2}$$

where

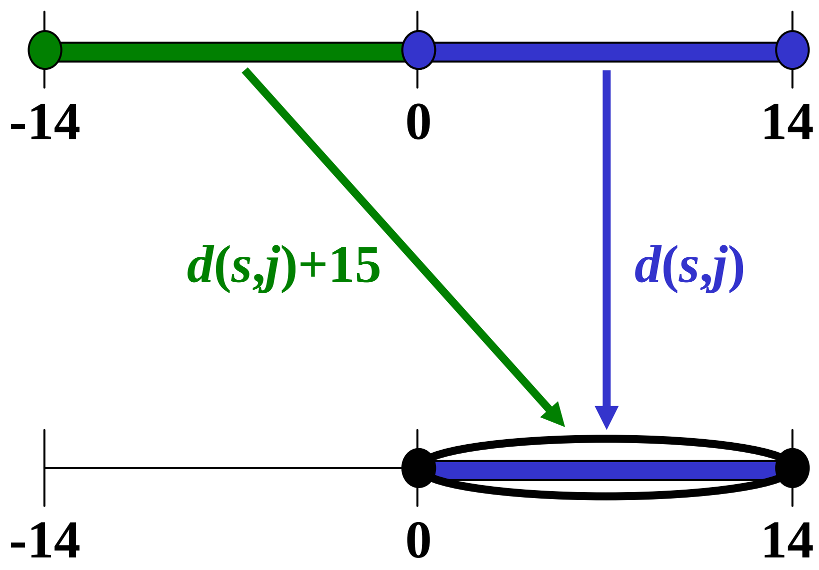
$$[e_j - e_{j+s}] = \begin{cases} 15-(e_j - e_{j+s}), & 8 \le e_j - e_{j+s} < 15 \\ e_j - e_{j+s}, & 0 < e_j - e_{j+s} < 8 \\ |e_j - e_{j+s}|, & -7 \le e_j - e_{j+s} < 0 \\ 15+(e_j - e_{j+s}), & -14 \le e_j - e_{j+s} < -7 \end{cases}$$

and

$$0 < [e_j - e_{j+s}] < 8.$$

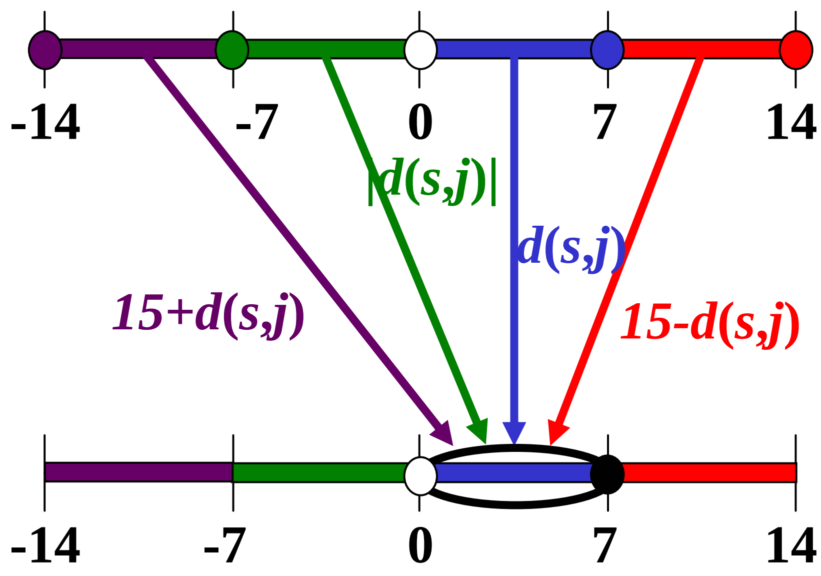
Illustration

Observe 15 elements of 15 × 15 sequence



Distinct modular differences property (mod 15)

Observe 8 elements of 15 × 15 sequence



Interesting property by Condition (2)

What it actually means

1 6 12 13 10 14 7 9 7 14 10 13 12 6 1

5 6 1 3 4 7 2 2 7 4 3 1 6 5

4 7 2 1 3 5   5 3 1 2 7 4

3 4 2 6 1   1 6 2 4 3

6 7 5 4   4 5 7 6

2 1 3   3 1 2

6 3   3 6

7   7

One necessary condition for "palindromes"

- Lemma : Let $\underline{\mathbf{e}} = (e_0,\ e_1,\ \cdots,\ e_{v-1})$ be a palindromic sequence of odd length v. If the sequence $\underline{\mathbf{e}}$ is a modular sonar sequence mod v, then the first $(v+1)/2$ terms satisfy the following:

$$\left|\{d(s,j)=[e_j-e_{j+s}]\neq 0 \mid 0\leq j<(v+1)/2-s\}\right|=(v+1)/2-s \quad \text{for all } 1\leq s<(v+1)/2$$

where

$$[e_j-e_{j+s}] = \begin{cases} v-(e_j-e_{j+s}), & (v+1)/2\leq e_j-e_{j+s}<v \\ e_j-e_{j+s}, & 0<e_j-e_{j+s}<(v+1)/2 \\ |e_j-e_{j+s}|, & -(v-1)/2\leq e_j-e_{j+s}<0 \\ v+(e_j-e_{j+s}), & -(v-1)\leq e_j-e_{j+s}<-(v-1)/2 \end{cases}$$

and

$$0<[e_j-e_{j+s}]<(v+1)/2.$$

Partial search for the case $v = 35$

- Search only for palindromic example of length 35 mod 35 using the necessary condition in the previous page.
- Runs a computer program a little more than a week, to conclude there are NONE.

Idea on algebraic construction (?)

- There exists n such that $v = p(p+2)$ is a divisor of $2^n - 1$.
- Consider the finite field of size 2^n and an element β of order v in it.
- Successive powers of β will produce a sequence of length v over $GF(2^n)$ or over $GF(2)^n$.
- Find a (potential) **transformation** that sends this sequence of binary n-tuples into that over the integers mod v, ***properly***.

35 divides 2^{12} - 1

- If a is primitive,
  then a^{117} has order 35.

$$
\begin{array}{ll}
\alpha^{117}(=\beta^{1}) : & 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1 \\
\alpha^{234}(=\beta^{2}) : & 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0 \\
\alpha^{351}(=\beta^{3}) : & 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1 \\
\alpha^{468}(=\beta^{4}) : & 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0 \\
\vdots & \vdots \\
\alpha^{3978}(=\beta^{34}) : & 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1 \\
\alpha^{4095}(=\beta^{35}) : & 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1
\end{array}
$$

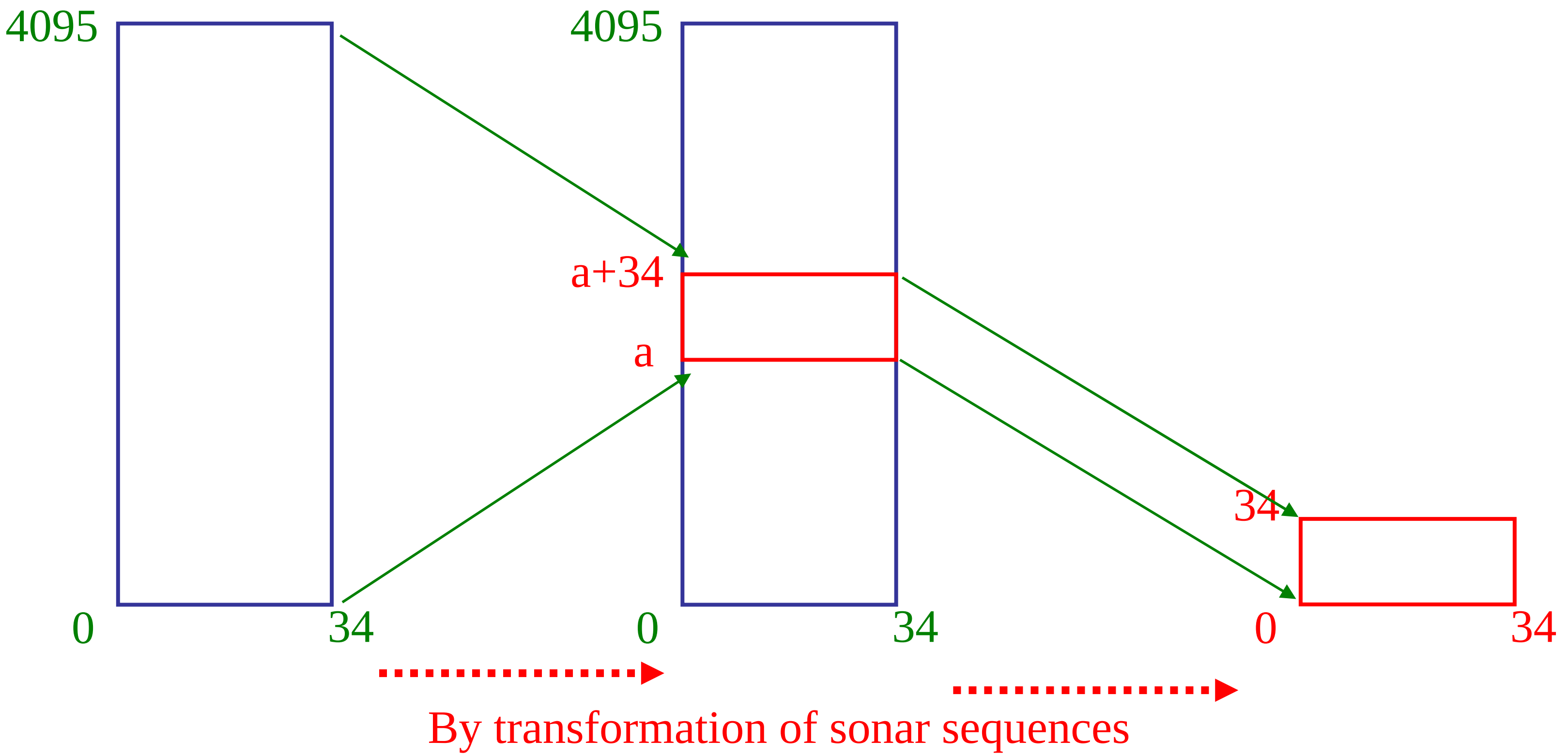
y_1 of $\underline{y}_1$

$\underline{x}_1$

$\underline{x}_2$

- modular sonar sequence of length 35 mod 4096:
  = (3417,1107,2707,1682,2516,413,1607,3489,1591,599,3075,2675,2390,3517,468,
  3268,532,1842,165,2947,3486,3124,1271,2954,899,199,2151,3684,3352,2647,
  346,3616,965,2863,2048)

SHEARING (?)



$2^{12} \times 35$ modular sonar sequence

35×35 modular sonar sequence

EXPANSION (??)