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......

- 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

Source of my travel money (sorry)
Coding and Information Theory Lab

A shift register (of degree n) is a "binary delay line" (with a "delay", i.e., binary storage) where at each stage a binary clock.
The contents of each stage is shifted to the next stage on the line.

If nothing is ever left the shift register, it will be empty (all 0s) again very fast.

In a binary clock feedback shift register, the contents of the next stage are stored "shifted", and this shift is used to shift the next stage of the shift register.
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 $10^4$: $v = 3439, 4355, 8591, 8835, 9135, 9215, \text{and } 9423$.

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

- Parts:
  - Two binary sequences of period $v$ with the ideal two-level autocorrelation
  - “shift sequence” $e$ of length $v$ defined over $\mathbb{Z}_v$

- Assembly:
  - Interleaved structure
“Shift sequence”

- The “shift sequence” $e = (e_0, e_1, \ldots, e_{v-1})$ over $\mathbb{Z}_v$ must satisfy the following:

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

- 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)

<table>
<thead>
<tr>
<th>e</th>
<th>1</th>
<th>3</th>
<th>1</th>
<th>7</th>
<th>11</th>
<th>3</th>
<th>14</th>
<th>15</th>
<th>8</th>
<th>8</th>
<th>13</th>
<th>7</th>
<th>4</th>
<th>14</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The sequence is represented with dots in the table, indicating the modular sonar sequence for a length of 15 and modulo 15.
## Real Motivation

<table>
<thead>
<tr>
<th>binary sequences of period $v$ with ideal two-level autocorrelation</th>
<th>$v \times v$ Modular sonar sequences (=“shift sequences”)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v = p$</td>
<td>$v = p$</td>
</tr>
<tr>
<td>$v = 2^n - 1$</td>
<td>$v = 2^n - 1$</td>
</tr>
<tr>
<td>$v = p(p + 2)$</td>
<td>???</td>
</tr>
</tbody>
</table>
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
  \[
g(i) = uf(i) + si + a \mod m
\]
- 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

<table>
<thead>
<tr>
<th>e</th>
<th>1</th>
<th>3</th>
<th>1</th>
<th>7</th>
<th>11</th>
<th>3</th>
<th>14</th>
<th>15</th>
<th>8</th>
<th>3</th>
<th>14</th>
<th>15</th>
<th>8</th>
<th>13</th>
<th>7</th>
<th>4</th>
<th>14</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>1</th>
<th>3</th>
<th>1</th>
<th>7</th>
<th>11</th>
<th>3</th>
<th>14</th>
<th>15</th>
<th>8</th>
<th>13</th>
<th>7</th>
<th>4</th>
<th>14</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>2</td>
<td>9</td>
<td>11</td>
<td>8</td>
<td>4</td>
<td>10</td>
<td>7</td>
<td>0</td>
<td>16</td>
<td>6</td>
<td>3</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td>0</td>
<td>11</td>
<td>5</td>
<td>4</td>
<td>10</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>10</td>
<td>1</td>
<td>9</td>
<td>16</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>16</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>2</td>
<td>7</td>
<td>3</td>
<td>10</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>16</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>16</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>1</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>9</td>
<td>4</td>
<td>10</td>
<td>0</td>
<td>7</td>
<td>16</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>12</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>12</td>
<td>3</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 1**
Representative of Class 2

Array form of 15x15 Modular Sonar sequence in Class 2

Modular difference Triangle of 15x15 Modular Sonar sequence in Class 2
Representative of Class 3

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

Modular difference Triangle of 15 x 15 Modular Sonar sequence in Class 3
Representative of Class 4

Array form of 15x15 Modular Sonar sequence in Class 4

Modular difference Triangle of 15x15 Modular Sonar sequence in Class 4
### Array form of 15 x 15 Modular Sonar sequence in Class 5

<table>
<thead>
<tr>
<th>1</th>
<th>6</th>
<th>12</th>
<th>13</th>
<th>10</th>
<th>14</th>
<th>7</th>
<th>9</th>
<th>7</th>
<th>14</th>
<th>10</th>
<th>13</th>
<th>12</th>
<th>6</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- 5
- 0

**Coding and Information Theory Lab**
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 $15 \times 15$ 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

Class 1 (1800 seq.)

Class 2 (1800 seq.)

Class 3 (1800 seq.)

Class 4 (1800 seq.)

Mirror image

Class 5 (840 seq.)

Class 5 (840 seq.)

Mirror image

Class 5 (120 seq.)

self-reciprocal = palindromic

(1,3,1,7,11,3,14,15,8,8,13,7,4,14,2)

(2,14,4,7,13,3,8,8,15,14,3,11,7,1,3)

(1,6,12,13,10,14,7,9,7,14,10,13,12,6,1)

(1,6,12,13,10,14,7,9,7,14,10,13,12,6,1)
Some property of Class 5

- 120 sequences in Class 5 are “palindrome”, that is,
  \[ f(i) = f(v - i), \quad 0 \leq i \leq v \]  
  (1)

- For any palindromic sequence in Class 5, the first 8 symbols satisfy:
  \[ \{d(s, j) = [e_j - e_{j+s}] \neq 0 \mid 0 \leq j < 8 - s\} = 8 - s \quad 1 \leq s < 8 \]  
  (2)

where

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

and

\[ 0 < [e_j - e_{j+s}] < 8. \]
Observe 15 elements of $15 \times 15$ sequence

Observe 8 elements of $15 \times 15$ sequence

Distinct modular differences property (mod 15)

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  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
7

Coding and Information Theory Lab
One necessary condition for “palindromes”

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

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

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 $\nu = 35$

- 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 $\nu = p(p + 2)$ is a divisor of $2^n - 1$.

- Consider the finite field of size $2^n$ and an element $\beta$ of order $\nu$ in it.

- Successive powers of $\beta$ will produce a sequence of length $\nu$ 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 $\nu$, properly.
35 divides $2^{12} - 1$

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

- 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 (?)

By transformation of sonar sequences

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

$35 \times 35$ modular sonar sequence
EXPANSION (??)

7x7