Sequences in Mobile Communication Systems

Mohsen Toorani

Department of Informatics
University of Bergen
May 2011
Outline

• Evolution of Mobile Networks (1G/2G/3G/4G)
• m-sequences and applications
• Pseudo-random Sequence Generators (PRSG)
• GSM and UMTS
• CDMA applications
• Spread Spectrum
Generation of Mobile Networks

1G \rightarrow 2G \rightarrow 2.5G \rightarrow 3G \rightarrow 3.5G \rightarrow 4G

AMPS/NTT/NMT \rightarrow GSM/D-AMPS/IS-95/PDC/PHS \rightarrow GPRS/EDGE/i-mode/WAP \rightarrow IMT-2000(W-CDMA/cdma2000) \rightarrow HDR/1xtreme

Voice Analog \rightarrow Voice over Circuit Switch

Data/Multimedia over Circuit Switch
- 9.6k – 28.8k – 64k – 384k – 2M

Data/Multimedia/Internet over IP
- 9.6k – 28.8k – 64k – 384k – 2M – 20M

All over IP
- 384k – 2M – 20M – 200M
Different Mobile Generations

Cellular Wireless Law of Speed vs. Decade

- **1G**: AMPS
- **2G**: GSM
- **3G**: UMTS
- **4G**: LTE
- **5G**: mobile device for everything

- **Mbps**
- **kbps**
- **bps**

- **Gbps**

- **10G**
- **100G**
- **1T**


- **Cell size shrinks**
- **Cell count increases**

30 Years
Real World Access Technology
Moving from Voice to Broadband with VoIP

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMPS, TACS, NMT</td>
<td>1G</td>
</tr>
<tr>
<td>LTE, WiMAX</td>
<td>2G</td>
</tr>
<tr>
<td>TDMA, PDC</td>
<td>3G</td>
</tr>
<tr>
<td>GPRS/EDGE</td>
<td>4G</td>
</tr>
</tbody>
</table>

User #1
User #2
User #3
User #4
Sequence Design in Communication Systems

**Sequence Design in Communication Systems for Reliability, Security and Availability**

- Information source
  - Format A/D
  - Source encode
  - Encrypt Authenticate
  - Channel encode
  - Multiplex
  - Modulation
  - Spread code generator

- Timing and synchronization
  - Spread spectrum modulation
  - Information channel (Internet, CD, atmosphere, ...)

- Format D/A
  - Source decode
  - Decrypt Verify
  - Channel decode
  - Demultiplex
  - Demodulation
  - Spread spectrum despread

- Information destination
  - To other destinations
  - Spread code generator
m-sequence

• Linear recurrent sequences having the biggest period \( L=p^{n-1} \) are called **Maximal-length Sequences** or **m-sequences**

• Linear recurrence: \( s_{t+n}+c_{n-1}s_{t+n-1}+...+c_0s_t = 0 \), \( c_i, s_i \in \text{GF}(p) \)

• Characteristic polynomial \( f(x)=x^n+c_{n-1}x^{n-1}+...+c_0 \)

\[
\begin{align*}
(s_t) & : 000100110101111 \\
(s_{t+4}) & = s_{t+1} + s_t \\
f(x) & = x^4+x+1
\end{align*}
\]
Applications of m-sequences

- Pseudo-random sequences
- Stream ciphers
- CDMA
- Spread Spectrum
- Radar
- Synchronization
- ...

Pseudo-random Sequence Generators (PRSG)

Three Periods of Research for Pseudo-Random Sequences:

• Period of pre-application (before 1948)
• Golden period of m-sequences (1948-1969)
• Period of non-linear generators (1969 - present)
Golden period of m-sequences (1948-1969)

- Shannon's Result (1948): One-time-pad is unbreakable
- Berlekamp-Massey algorithm (1969)

LFSR generates $m$-sequences

= Maximal length sequences
= Pseudo-noise (PN) sequences
Period of Non-Linear Generators (1969 - present)

• Design towards 2-Level Autocorrelation and Low Cross Correlation

• Design towards Large Linear Span

LFSR used as the Basic Block
2-Level Autocorrelation Sequences
(Orthogonal codes)

- PN-sequences = $m$-sequences (1931, Singer, 1958, Golomb)
- Hyper-oval Construction (Maschietti: 1998)
- Kasami Power Function Construction (Dobbertin, Dillon, 1998)
Low Cross Correlation

Pseudo-random sequence generators adopted by 2G and 3G:

- Hadamard Sequences (2-level autocorrelation Sequences)
- Gold-pair Sequences (1967)
- Kasami Sequences (1970)
- $\mathbb{Z}_4$ Sequences (1996, Kumar-Helleseth-Calderbank-Hammons)
Known Approaches for Design of PRSG based on LFSRs

• M-Sequences (1948-1969)
• Filter Function Generators (Key: 1973)
• Combinatorial Function Generators (Groth: 1971)
• Clock Controlled Generators (Beth-Piper: 1984)
• Shrinking Generators (Coppersmith-Krawczys-Mansour, 1993)
Applications of PRSG

- Key Stream Generators in Stream cipher Models in Wireless Environment
- Functions in Block Ciphers
- Session Key Generators
- Pseudo-random Number Generators in Digital Signature Standard (DSS), EC-DSS, etc.
- Digital Watermark
- Multimedia Encryption
- Low-cost encryption
- ....
Stream Ciphers

- A5/1 & A5/2 in GSM (2G)
- RC4 in Web Security & SSL
- E0 in Bluetooth Standard
- ...
GSM (2G)

- 3.5 billion of the world’s 4.3 billion mobile subscribers use GSM (A5/1 & A5/2)
- A5/2 is a deliberately weakened version of A5/1 (for other countries)
A5/1

Consists of 3 LFSRs of different lengths

- **19 bits**
  - $x^{18} + x^{17} + x^{16} + x^{13} + 1$
  - clock bit 8
  - tapped bits: 13, 16, 17, 18

- **22 bits**
  - $x^{21} + x^{20} + 1$
  - clock bit 10
  - tapped bits 20, 21

- **23 bits**
  - $x^{22} + x^{21} + x^{20} + x^{7} + 1$
  - clock bit 10
  - tapped bits 7, 20, 21, 22
Some attacks to A5/1

<table>
<thead>
<tr>
<th>Attacker</th>
<th>Year</th>
<th>Attack Type</th>
<th>Pre-Proc. Steps</th>
<th>Available Data</th>
<th>Storage</th>
<th>Attack Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Golic</td>
<td>1997</td>
<td>Solving Linear Eqns.</td>
<td>$2^{40.16}$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Golic</td>
<td>1997</td>
<td>Solving Linear Eqns.</td>
<td>$2^{40.16}$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biryukov et al.</td>
<td>2000</td>
<td>Time-memory trade off</td>
<td>$2^{48}$</td>
<td>2 mins.</td>
<td>300 GB</td>
<td>1 second</td>
</tr>
<tr>
<td>Biryukov et al.</td>
<td>2000</td>
<td>Random Subgraph</td>
<td>$2^{48}$</td>
<td>2 secs.</td>
<td>300 GB</td>
<td>Several Mins.</td>
</tr>
<tr>
<td>Biham et al.</td>
<td>2000</td>
<td></td>
<td>$2^{38}$</td>
<td>$2^{20.8}$ bits</td>
<td>32 GB</td>
<td>$2^{39.91}$ clockings</td>
</tr>
<tr>
<td>Ekdahl et al.</td>
<td>2003</td>
<td>No initialization</td>
<td>No</td>
<td>2-5 mins.</td>
<td></td>
<td>Few mins.</td>
</tr>
<tr>
<td>Maximov et al.</td>
<td>2004</td>
<td>Improved Ekdahl et al.</td>
<td>No</td>
<td>A few secs.</td>
<td></td>
<td>Less than 1 min</td>
</tr>
</tbody>
</table>
UMTS (3G)

Confidentiality in UMTS
Gold sequence generator used in UMTS on the downlink for generating of scrambling codes
CDMA

- **FDMA (Frequency Division Multiple Access)**
  Each user uses a different frequency

- **TDMA (Time Division Multiple Access)**
  Users are on different timeslots

- **CDMA (Code Division Multiple Access)**
  Each user uses the same frequency all the time
CDMA (Encode/Decode)
CDMA with two users

senders

\[ Z_{i,m} = d_i \cdot c_m \]

channel, \( Z_{i,m}^* \)

\[ d_i = \sum_{m=1}^{M} Z_{i,m}^* \cdot c_m \]

receiver 1
CDMA

Channelization coding and scrambling in CDMA systems
(when one transmitter needs to transmit several channels simultaneously)
CDMA Evolution Paths

- CDMA IS-95
- CDMA 1xRTT
- CDMA 1xEV-DO
- CDMA 1xEV-DV

9.6kbps -> 153.6kbps

2G  2.5G  3G

2Mbps
CDMA Advantages

- Spread Spectrum
- Soft & Softer Handoff
- Rake Receiver
- Variable Rate Vocoder
- High quality voice
- Power Control
- Coverage
- Simple Network Planning
- Green Handset
- Smooth migration to 3G and the operator’s benefit is protected at the most
IS-95

- IS-95 Downlink
cdma2000 Downlink Modulation

\[ \sum \]

other channels \( X_I \)

Walsh code

QOF code

\[ Y_I \]

\[ Y_Q \]

other channels \( X_Q \)

phase rotate for QOF

+ \[ + \] \[- \]

pulse shape

\[ \cos(\omega_c t) \]

\[ \sin(\omega_c t) \]
Walsh sequences

<table>
<thead>
<tr>
<th>Index integer $j$</th>
<th>Index sequence</th>
<th>Walsh sequences of order $8 = 2^3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>$W_0 = 00000000$</td>
</tr>
<tr>
<td>1</td>
<td>001</td>
<td>$W_1 = 00001111$</td>
</tr>
<tr>
<td>2</td>
<td>010</td>
<td>$W_2 = 00111100$</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>$W_3 = 00110011$</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>$W_4 = 01100110$</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>$W_5 = 01101001$</td>
</tr>
<tr>
<td>6</td>
<td>110</td>
<td>$W_6 = 01011010$</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>$W_7 = 01010101$</td>
</tr>
</tbody>
</table>

**Walsh Sequence of Order 8**

+1 → “0”
-1 → “1”

**Walsh Functions of order 8**
Long PN Sequence
(IS-95)

• A “long” PN sequence (r =42) is used to scramble the user data with a different code shift for each user

• The 42-degree characteristic polynomial is given by:
  \[ x^{42} + x^{41} + x^{40} + x^{39} + x^{37} + x^{36} + x^{35} + x^{32} + x^{26} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{11} + x^9 + x^7 + 1 \]

• The period of the long code is \( 2^{42} - 1 \approx 4.4 \times 10^2 \) chips and lasts over 41 days
Short PN Sequences
(IS-95)

• Two “short” PN sequences (r=15) are used to spread the quadrature components of the forward and reverse link waveforms.

• They can be considered a two-dimensional binary vector with distinct I and Q component sequences.

• The characteristic polynomials are given by:
  – $x^{15}+x^{10}+x^8+x^7+x^6+x^2+x$ (I-channel)
  – $x^{15}+x^{12}+x^{11}+x^{10}+x^9+x^5+x^4+x^3+1$ (Q-channel)

• The period of the short code is:
  $2^{15} - 1 = 32767$ chips $\equiv 80/3$ ms
# CDMA Code Summary

<table>
<thead>
<tr>
<th>Type of Sequence</th>
<th>How Many</th>
<th>Length</th>
<th>Special Properties</th>
<th>Forward Link Function</th>
<th>Reverse Link Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walsh Codes/Sequences</td>
<td>64</td>
<td>64 chips 1/19,200 sec.</td>
<td>Mutually Orthogonal</td>
<td>User identity within cell’s signal</td>
<td>Orthogonal Modulation (information carrier)</td>
</tr>
<tr>
<td>Short PN Sequences</td>
<td>2</td>
<td>32,768 chips 26-2/3 ms 75x in 2 sec.</td>
<td>Orthogonal with itself at any time shift value except 0</td>
<td>Distinguish Cells &amp; Sectors</td>
<td>Quadrature Spreading (Zero offset)</td>
</tr>
<tr>
<td>Long PN Sequences</td>
<td>1</td>
<td>$2^{62}$ chips ~41 days</td>
<td>near-orthogonal if shifted</td>
<td>Data Scrambling to avoid strings of 1’s or 0’s</td>
<td>Distinguish users</td>
</tr>
</tbody>
</table>

- **Orthogonality**
  - Walsh Codes/Sequences: 64 mutually orthogonal.
  - Short PN Sequences: Orthogonal with itself except at shift value 0.
  - Long PN Sequences: near-orthogonal if shifted.

- **Modulation**
  - Walsh Codes/Sequences: Orthogonal Modulation (information carrier).
  - Short PN Sequences: Quadrature Spreading (Zero offset).
  - Long PN Sequences: Data Scrambling to avoid strings of 1’s or 0’s.

- **User Identity**
  - Walsh Codes/Sequences: User identity within cell’s signal.
  - Short PN Sequences: Distinguish Users.

- **Signal Distinguish**
  - Walsh Codes/Sequences: Cells & Sectors.
  - Short PN Sequences: Distinguish Cells & Sectors.
  - Long PN Sequences: Distinguish Users.

- **Time Duration**
  - Short PN Sequences: 26-2/3 ms.
  - Long PN Sequences: ~41 days.
Spread Spectrum

SS is typically implemented in one of two forms:

• **Direct Sequence Spread Spectrum (DSSS):** The modulated data signal is multiplied by a wideband spreading signal/code.

• **Frequency hopping Spread Spectrum (FHSS):** hops the modulated data signal over a wide bandwidth by hanging its carrier frequency according to a spreading code.
Spread Spectrum

Frequency Hopping

$B_c$

$B$

$f_0$, $f_1$, $f_2$, $f_3$, $f_4$, $f_5$, $f_6$, $f_7$, $f_8$, $f_9$
Spread Spectrum

Illustration of spreading and despreading
Spread Spectrum

Basic Spread spectrum communication system
Spread Spectrum
(Generation of Spreading Codes)
Spread Spectrum (DSSS)

Synchronization Loop for Direct Sequence Spread Spectrum (DSSS)
Spread Spectrum (FHSS)

Frequency Hoping Spread Spectrum (FHSS) System Model
Conclusion

• Sequences / M-sequences have many applications in mobile communication systems.
• Pseudo-random sequences, Stream ciphers and CDMA are some examples with many applications in different mobile communication systems.
• There are other applications that are not considered in this brief review.