Short and Efficient Frequency Hopping Codes

Young-Joon Kim, Dae-Son Kim and Hong-Yeop Song

{yj.kim, ds.kim, hysong}@yonsei.ac.kr
Coding and Information Theory Lab
Yonsei University, Seoul, KOREA

The 2006 International Symposium on Information Theory and its Applications,
October 29 - November 1, 2006, COEX, Seoul, Korea

Outline

Outline

Features of FH-SS

- Anti-Jamming
- Processing Gain
- Frequency Diversity (Fast FH)
- Combat to multi-path fading
- Dependent on Frequency Hopping Codes Design

General Requirements for Hopping Sequences

- Spectrum Spreading
  - Long Period, Large number of Hopping Symbol
- Acquisition/Synchronization
  - Good Hamming Auto-Correlation
- Multiple Access
  - Large Number of Hopping Symbol, Good Hamming Cross-Correlation
- Security
  - Large Linear Complexity

General Requirements for Hopping Sequences

- Spectrum Spreading
  - Long Period, Large number of Hopping Symbol
- Acquisition/Synchronization
  - Good Hamming Auto-Correlation
- Multiple Access
  - Large Number of Hopping Symbol, Good Hamming Cross-Correlation
- Security
  - Large Linear Complexity

General Requirements for Hopping Sequences

- Spectrum Spreading
  - Long Period, Large number of Hopping Symbol
- Acquisition/Synchronization
  - Good Hamming Auto-Correlation
- Multiple Access
  - Large Number of Hopping Symbol, Good Hamming Cross-Correlation
- Security
  - Large Linear Complexity

General Requirements for Hopping Sequences

- Spectrum Spreading
  - Long Period, Large number of Hopping Symbol
- Acquisition/Synchronization
  - Good Hamming Auto-Correlation
- Multiple Access
  - Large Number of Hopping Symbol, Good Hamming Cross-Correlation
- Security
  - Large Linear Complexity

Requirements for Short Hopping Sequences

- Short length for synchronization only
  - Memory Based Sequence
  - Security (don't care!)
  - Balance
  - Good Hamming Auto-correlation

Requirements for Short Hopping Sequences

- Short length for synchronization only
  - Memory Based Sequence
  - Security (don't care!)
  - Balance
  - Good Hamming Auto-correlation

Outline

- Starting with Perfect Balanced Sequence

Balance-Construction 1

- Example
  - $p = 13, q = 3, \mu = 2$

n	0	1	2	3	4	5	6	7	8	9	10	11
2^n	1	2	4	8	3	6	12	11	9	5	10	7
$a(n)$	1	2	1	2	0	0	0	2	0	2	1	1

- Construction 1 sequence
  - p : a prime
  - q : a divisor of $p-1$
  - μ : a primitive root (mod p)
  - $a(n) = \mu^n \pmod{q}, \quad n = 0, \ldots, p-2$
  - Balanced !

Hamming Autocorrelation of Construction 1

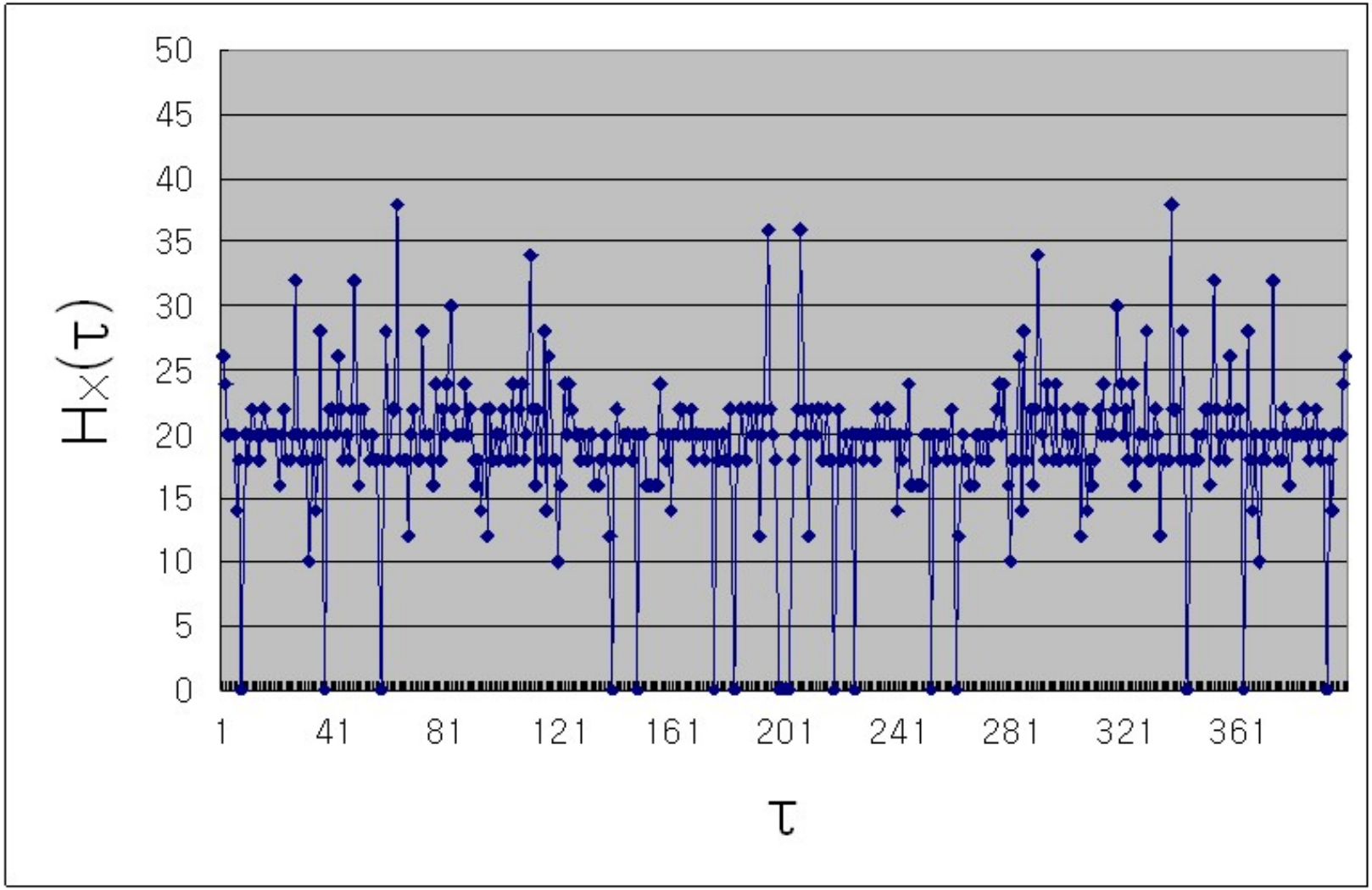

Figure: Hamming autocorrelation of Construction 1 Sequence ($p = 401$, $q = 20$)

- Starting with Perfect Hamming Autocorrelation

Hamming Autocorrelation-Power Residue Sequences

- Example
  - $p = 13, q = 3, \mu = 2$

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

  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

- Power Residue Sequences (PRS)
  - p, q : a prime, a divisor of $p-1$
  - μ : a primitive root (mod p)
  - Coset partitioning : $C_k = \mu^k \cdot C_0$, C_0=a set of q-th power residues (mod p)
  - $$s(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ k, & \text{if } n \in C_k \text{ for } k \in \mathbb{Z}_q \end{cases}$$
  - Perfect Hamming Auto-correlation
  - Length : not $p-1$ but p

Hamming Autocorrelation-Power Residue Sequences

- Example
  - $p = 13, q = 3, \mu = 2$

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

  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

- Power Residue Sequences (PRS)
  - p, q : a prime, a divisor of $p-1$
  - μ : a primitive root (mod p)
  - Coset partitioning : $C_k = \mu^k \cdot C_0$, C_0=a set of q-th power residues (mod p)
  - $$s(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ k, & \text{if } n \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$
  - Perfect Hamming Auto-correlation
  - Length : not $p-1$ but p

Hamming Autocorrelation-Power Residue Sequences

- Example
  - $p = 13, q = 3, \mu = 2$

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

  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

- Power Residue Sequences (PRS)
  - p, q : a prime, a divisor of $p-1$
  - μ : a primitive root (mod p)
  - Coset partitioning : $C_k = \mu^k \cdot C_0$, C_0=a set of q-th power residues (mod p)
  - $$s(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ k, & \text{if } n \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$
  - Perfect Hamming Auto-correlation
  - Length : not $p-1$ but p

Hamming Autocorrelation-Power Residue Sequences

- Example
  - $p = 13, q = 3, \mu = 2$

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

  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

- Power Residue Sequences (PRS)
  - p, q : a prime, a divisor of $p-1$
  - μ : a primitive root (mod p)
  - Coset partitioning : $C_k = \mu^k \cdot C_0$, C_0=a set of q-th power residues (mod p)
  - $$s(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ k, & \text{if } n \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$
  - Perfect Hamming Auto-correlation
  - Length : not $p-1$ but p

Hamming Autocorrelation-Power Residue Sequences

- Example
  - $p = 13, q = 3, \mu = 2$

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

  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$s(n)$	0	0	1	1	2	0	2	2	0	2	1	1	0

- Power Residue Sequences (PRS)
  - p, q : a prime, a divisor of $p-1$
  - μ : a primitive root (mod p)
  - Coset partitioning : $C_k = \mu^k \cdot C_0$, C_0=a set of q-th power residues (mod p)
  - $$s(n) = \begin{cases} 0, & \text{if } n \equiv 0 \bmod p, \\ k, & \text{if } n \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$
  - Perfect Hamming Auto-correlation
  - Length : not $p-1$ but p

Hamming Autocorrelation-Construction 2

- Example
  - $p = 13, q = 3, \mu = 2$

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	0	1	1	2	0	2	2	0	2	1	1	0

- Construction 2 - Initial Position Deleted PRS
  - Length : $p-1$
  - Perfect Balanced
  - How good the resulting sequence is in terms of Hamming auto-correlation?

Hamming Autocorrelation-Construction 2

- Example
  - $p = 13, q = 3, \mu = 2$

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	0	1	1	2	0	2	2	0	2	1	1	0

- Construction 2 - Initial Position Deleted PRS
  - Length : $p-1$
  - Perfect Balanced
  - How good the resulting sequence is in terms of Hamming auto-correlation?

Hamming Autocorrelation-Construction 2

- Example
  - $p = 13, q = 3, \mu = 2$

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	0	1	1	2	0	2	2	0	2	1	1	0

- Construction 2 - Initial Position Deleted PRS
  - Length : $p-1$
  - Perfect Balanced
  - How good the resulting sequence is in terms of Hamming auto-correlation?

Hamming Autocorrelation-Construction 2

- Example
  - $p = 13, q = 3, \mu = 2$

n	1	2	3	4	5	6	7	8	9	10	11	12
$b(n)$	0	1	1	2	0	2	2	0	2	1	1	0

- Construction 2 - Initial Position Deleted PRS
  - Length : $p-1$
  - Perfect Balanced
  - How good the resulting sequence is in terms of Hamming auto-correlation?

Hamming Autocorrelation of Construction 2

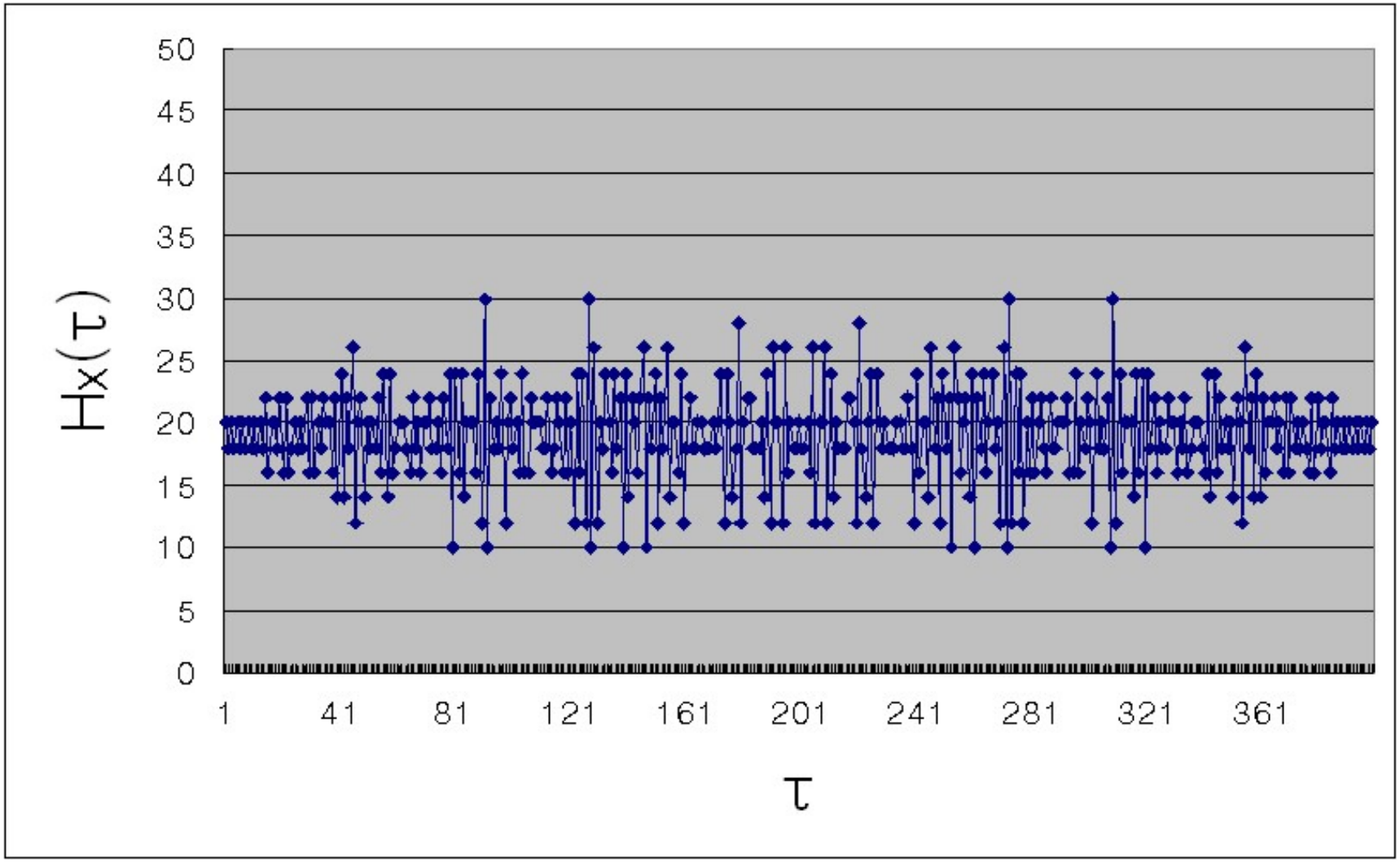

Figure: Hamming autocorrelation of Construction 2 Sequence ($p = 401$, $q = 20$)

Hamming Autocorrelation-Construction 3

- Example
  - $p = 13, q = 3, \mu = 2$

delete position	0	1	2	3	4	5	6	7	8	9	10	11	12
H_{max}	4	4	4	4	5	6	6	6	6	5	4	4	4

  - Optimal Positions : 0, 1, 2, 3, 10, 11, 12

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$c(n)$	0	del	1	1	2	0	2	2	0	2	1	1	0

- Construction 3 - Optimal Position Deleted PRS
  - Optimal positions : resulting deleted PRS gives the lowest maximum Hamming autocorrelation
  - Length : $p-1$
  - Almost Balanced

Hamming Autocorrelation-Construction 3

- Example
  - $p = 13, q = 3, \mu = 2$

delete position	0	1	2	3	4	5	6	7	8	9	10	11	12
H_{max}	4	4	4	4	5	6	6	6	6	5	4	4	4

  - Optimal Positions : 0, 1, 2, 3, 10, 11, 12

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$c(n)$	0	del	1	1	2	0	2	2	0	2	1	1	0

- Construction 3 - Optimal Position Deleted PRS
  - Optimal positions : resulting deleted PRS gives the lowest maximum Hamming autocorrelation
  - Length : $p-1$
  - Almost Balanced

Hamming Autocorrelation-Construction 3

- Example
  - $p = 13, q = 3, \mu = 2$

delete position	0	1	2	3	4	5	6	7	8	9	10	11	12
H_{max}	4	4	4	4	5	6	6	6	6	5	4	4	4

  - Optimal Positions : 0, 1, 2, 3, 10, 11, 12

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$c(n)$	0	del	1	1	2	0	2	2	0	2	1	1	0

- Construction 3 - Optimal Position Deleted PRS
  - Optimal positions : resulting deleted PRS gives the lowest maximum Hamming autocorrelation
  - Length : $p-1$
  - Almost Balanced

Hamming Autocorrelation of Construction 3

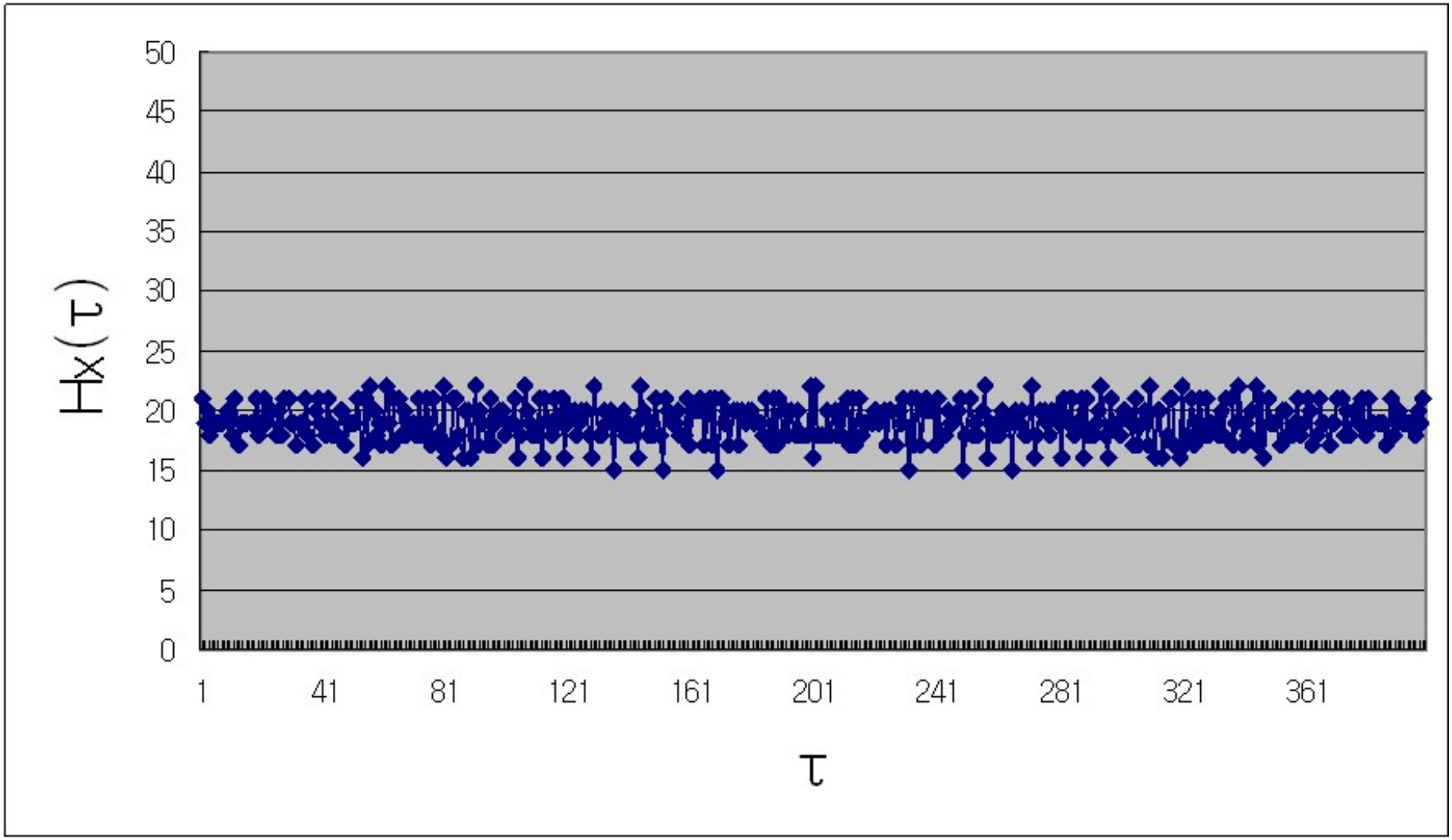

Figure: Hamming autocorrelation of Construction 3 Sequence ($p = 401$, $q = 20$)

EXTRA-Sidel'nikov Sequences

- Example
  - $p = 13, q = 3, \mu = 2$
  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^n = 1$	2	3	5	9	4	7	0	12	10	6	11	8
$t(n)$	1	1	0	2	2	2	0	0	1	2	1	0

- Sidel'nikov Sequences
  - Length : $p^m - 1$, (p : a prime)
  - q : a divisor of $p^m - 1$
  - μ : a primitive element in $GF(p^m)$
  - $$t(n) = \begin{cases} 0, & \text{if } \mu^n + 1 \equiv 0 \\ k, & \text{if } \mu^n + 1 \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$

    where $C_k = \mu^k \cdot C_0$ and C_0=a set of q-th power residues in $GF(p^m)$
  - Perfect Hamming Auto-correlation, Balanced

EXTRA-Sidel'nikov Sequences

- Example
  - $p = 13, q = 3, \mu = 2$
  - $C_0 = \{1,5,8,12\}$, $C_1 = 2 \cdot C_0 = \{2,10,3,11\}$ and $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

n	0	1	2	3	4	5	6	7	8	9	10	11
$2^n = 1$	2	3	5	9	4	7	0	12	10	6	11	8
$t(n)$	1	1	0	2	2	2	0	0	1	2	1	0

- Sidel'nikov Sequences
  - Length : $p^m - 1$, (p : a prime)
  - q : a divisor of $p^m - 1$
  - μ : a primitive element in $GF(p^m)$
  - $$t(n) = \begin{cases} 0, & \text{if } \mu^n + 1 \equiv 0 \\ k, & \text{if } \mu^n + 1 \in C_k \text{ for } k \in \mathbf{Z}_q \end{cases}$$

    where $C_k = \mu^k \cdot C_0$ and C_0=a set of q-th power residues in $GF(p^m)$
  - Perfect Hamming Auto-correlation, Balanced

Hamming Autocorrelation of Sidel'nikov sequence

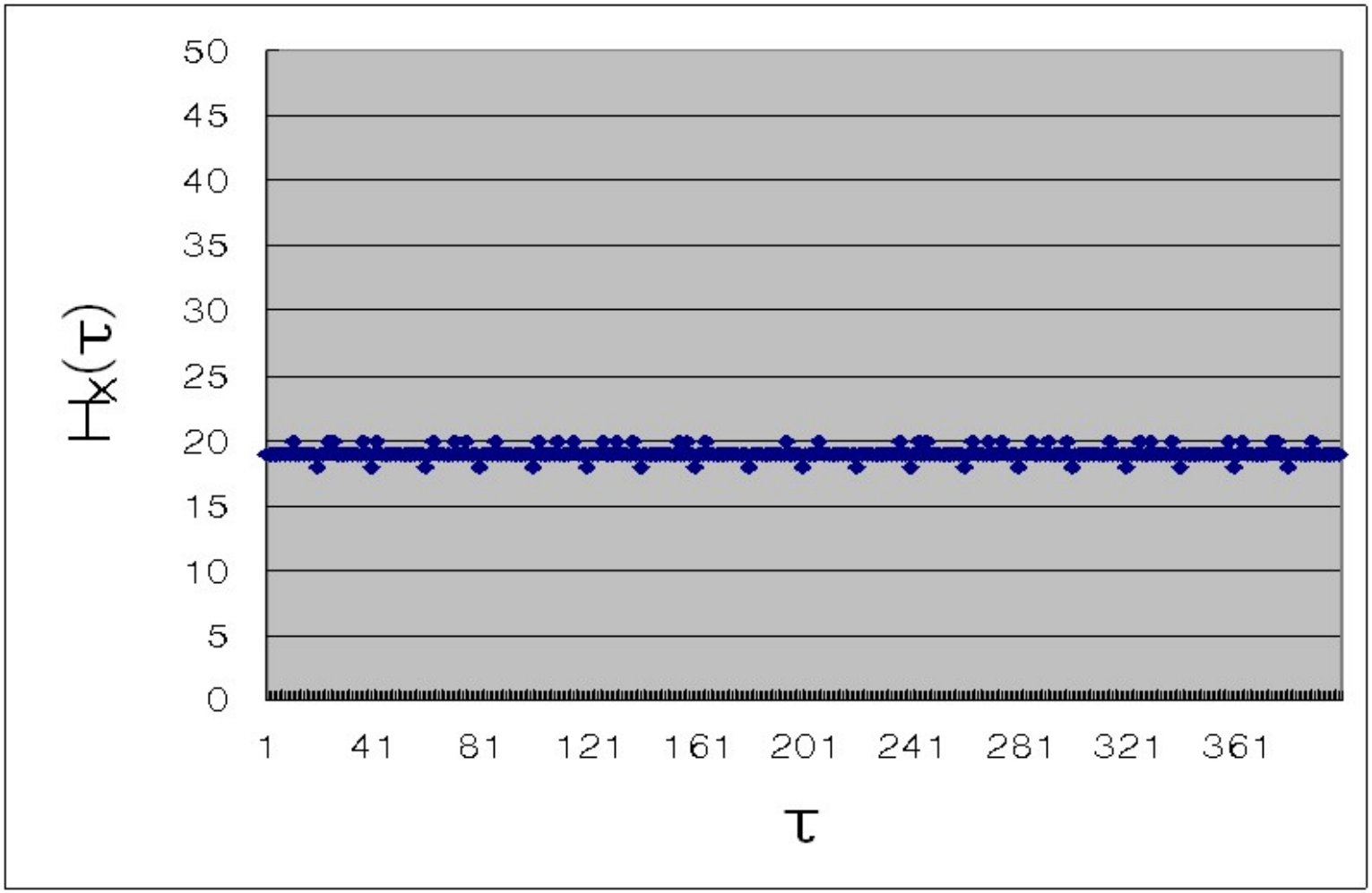

Figure: Hamming autocorrelation of Sidel'nikov Sequence ($p = 401$, $q = 20$)

Outline

Hamming Autocorrelation Comparison

- Hamming autocorrelation Comparison $(100 < p < 300$ and $10|(p-1)$

p-1	q	Hmax of Construction 1	Hmax of Construction 2	Hmax of Construction 3	Hmax of Sidel'nikov	Lower Bound of Hmax
100	10	18	16	12	10	10
130	10	22	20	15	14	13
150	10	26	22	17	16	14
180	10	32	30	21	18	18
190	10	34	24	22	20	19
210	10	38	30	23	22	21
240	10	42	32	26	24	24
250	10	44	34	28	26	25
270	10	48	36	30	28	27
280	10	50	36	31	28	28

Outline

Summary

- It's not a theoretical result but an engineering approach
- A single short sequence for synchronization
- Future Work
  - Theoretical Analysis
  - In case of 'Length $\neq p^m - 1$'

Summary

- It's not a theoretical result but an engineering approach
- A single short sequence for synchronization
- Future Work
  - Theoretical Analysis
  - In case of 'Length $\neq p^m - 1$'