Short and Efficient Frequency Hopping Codes

April 28, 2006

Young-Joon Kim*, Dae-Son Kim

and Hong-Yeop Song

({yj.kim*, ds.kim, hy.song}@coding.yonsei.ac.kr)

Coding and Information Theory Lab

YONSEI University, Seoul, Korea

Contents

- Introduction
- Constructions of Proposed Sequences
  - Known Result - One Coincidence Set of Sequences
    - Construction 1
  - Known Result - Power Residue Sequences
    - Construction 2
    - Construction 3
- Hamming Autocorrelation Comparison of Proposed Sequences
- Conclusion

Introduction

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

Requirements for Short Hopping Sequences

- 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)
- Short Hopping Sequences
  - Memory Based Sequence
  - Balance
  - Good Hamming Autocorrelation

Known Results
- One Coincidence Set of Sequences*

- Let p be a prime. Let μ be a primitive root in Z_p.
  A set S=$\{s_j \mid 0 \le j \le p\text{-}1\}$, where s_j =$\{\mu^n + j \mod p \mid 0 \le n \le p\text{-}2\}$

  - Multiple access, Hamming auto/cross-correlation ≤ 1

- Example (p =7, and μ =3)

n	0	1	2	3	4	5
$s_0(n) = \mu^n + 0$	1	3	2	6	4	5
$s_1(n) = \mu^n + 1$	2	4	3	0	5	6
$s_2(n) = \mu^n + 2$	3	5	4	1	6	0
$s_3(n) = \mu^n + 3$	4	6	5	2	0	1
$s_4(n) = \mu^n + 4$	5	0	6	3	1	2
$s_5(n) = \mu^n + 5$	6	1	0	4	2	3
$s_6(n) = \mu^n + 6$	0	2	1	5	3	4

* A.A.Shaar and P.A.Davies, 'A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems,' IEE Proc. Vol. 131, Pt.F, No.7, Dec 1984
* McEliece, R.J., 'Some Combinatorial aspects of spread spectrum communication systems', in SKWIRZYNSKI, J.K. (Ed.)

Construction 1

- Construction 1 :
  - Length : p-1, where p is a prime
  - q : a divisor of p-1.

$$a(n) = s_0(n) \bmod q = \mu^n \bmod q \ , \ n=0,1,\ldots,p-2$$

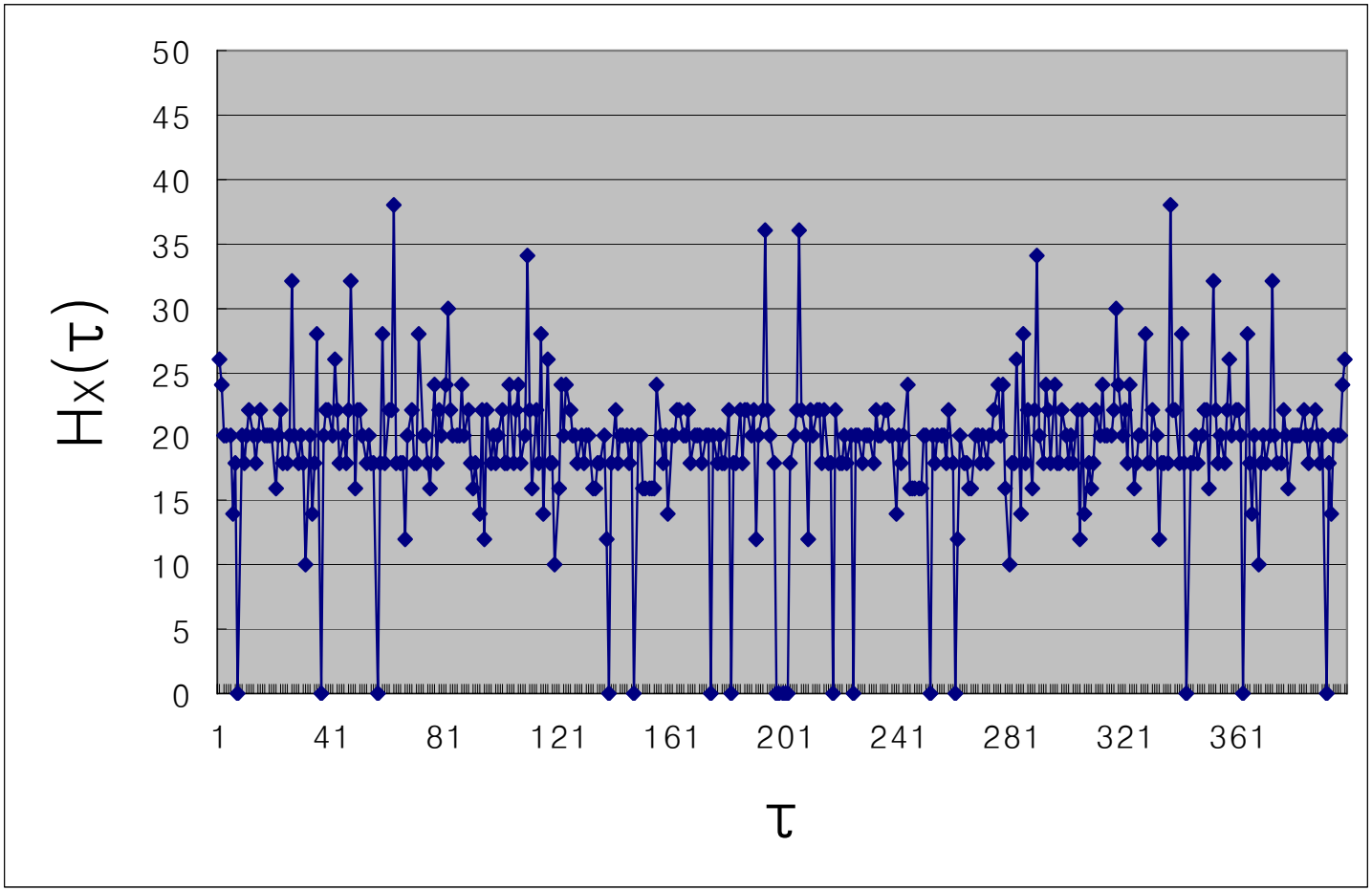
  - Balanced

- Example (p =13, q =3 and μ =2)

n	0	1	2	3	4	5	6	7	8	9	10	11
μ^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

Hamming Autocorrelation of Construction 1

- When p =401, q =20 and μ =3



Known Results
- Power Residue Sequences (PRS)

- Power Residue Sequences :
  - Length: a prime p
  - q : a divisor of p-1

$$t(n) = \begin{cases} 0, & \text{if } n = 0 \\ k, & \text{if } n \in C_k,\ 0 \le k < q \end{cases}$$

where, C_0 is a set of q th residues mod p and $C_i = \mu^i \cdot C_0$ for $1 \le i \le q$-1

  - Perfect Hamming Autocorrelation**

- Example (p =13, q =3 and μ =2)

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

**V.M.Sidelnikov, "Some k-valued pseudo-random and nearly equidistant codes," *Probl. Pered. Inform.*, Vol. 5, no. 1, pp. 16-22, 1969

Construction 2 (First Position-Deleted PRS)

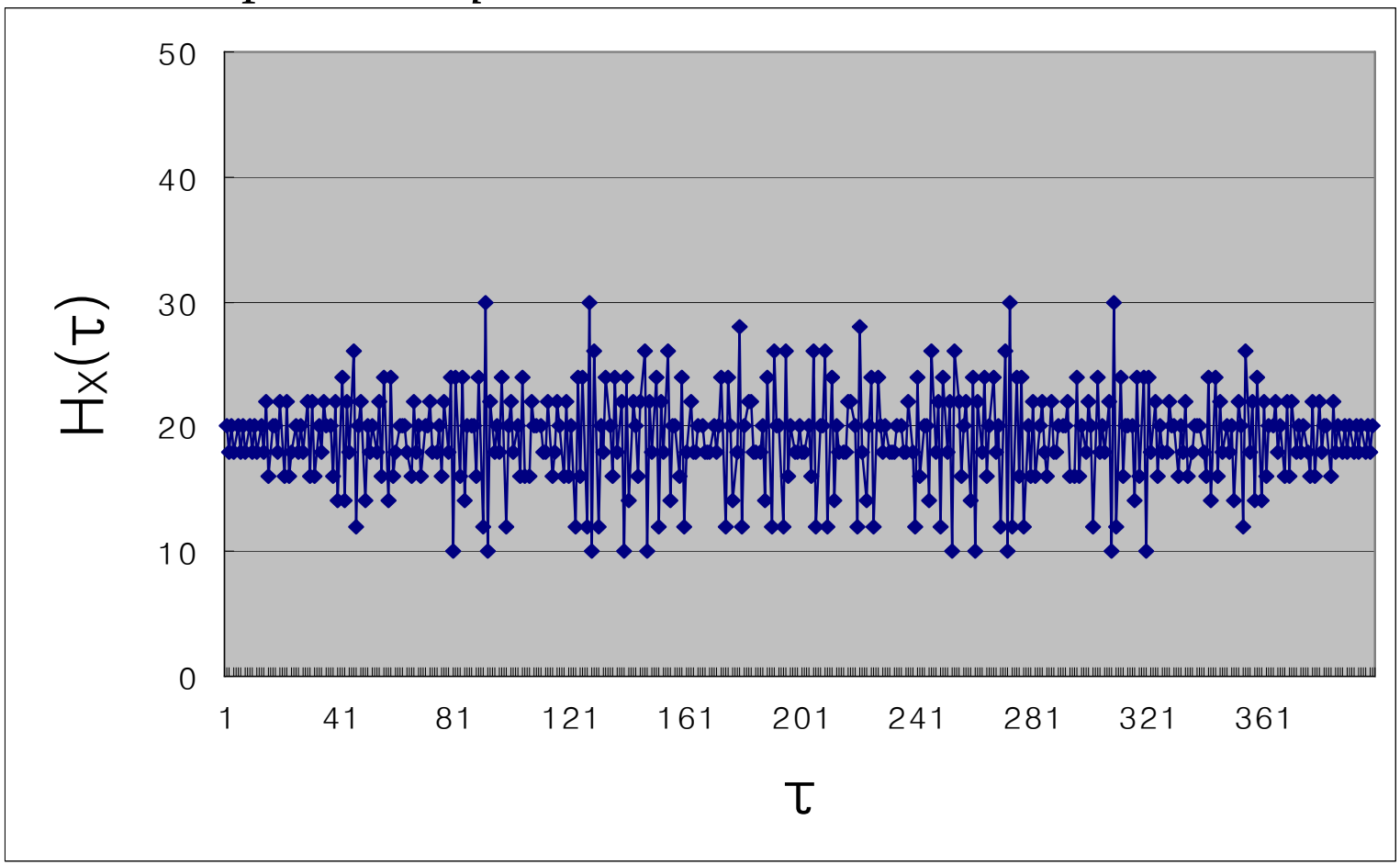
- Construction 2 : length p-1, where p is a prime
  - First position deleted sequence in the construction B
  - Balanced

- Example (p =13, q =3 and μ =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

Hamming Autocorrelation of Construction 2

- When p =401, q =20 and μ =3



Construction 3

- Construction 3 : length p-1, where p is a prime
  - Optimal position deleted sequence in the construction of PRS
  - Almost balanced

- Example (p =13, q =3 and μ =2)

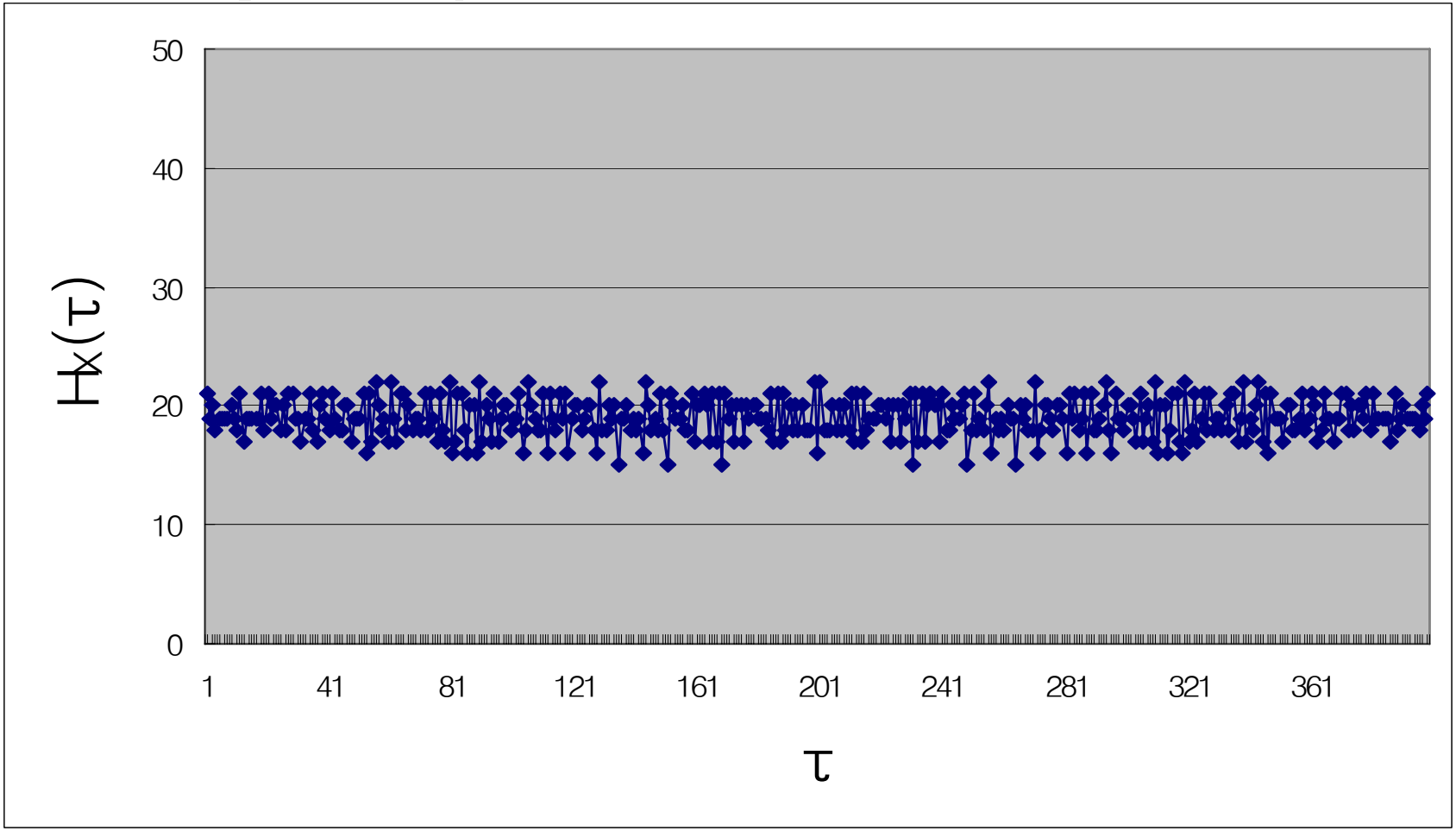
deleted position	0	1	2	3	4	5	6	7	8	9	10	11	12
H_{max}	4	4	4	4	5	6	6	6	6	5	4	4	4

optimal positions : 0, 1, 2, 3, 10, 11, 12

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

Hamming Autocorrelation of Construction 3

- When p =401, q =20 and μ =3



Hamming Autocorrelation Comparison

- When $100 < p < 300$ and p-1 is a multiple of 10

p	q	Hmax of Construction 1	Hmax of Construction 2	Hmax of Construction 3	Lower Bound of Hmax
101	10	18	16	12	10
131	10	22	20	15	13
151	10	26	22	17	14
181	10	32	30	21	18
191	10	34	24	22	19
211	10	38	30	23	21
241	10	42	32	26	24
251	10	44	34	28	25
271	10	48	36	30	27
281	10	50	36	31	28

Conclusion

- Three constructions of the short hopping sequences for the hopping system
- Comparison of proposed sequences
  - Balance
  - Hamming autocorrelation
- Further Work
  - How to construct the sequences in the cases of ‘length+1$\not\equiv$0 mod p’