Frequency Hopping Sequences with Optimal Partial Autocorrelation Properties

July 1, 2004.

Yu-Chang Eun, Seok-Yong Jin, Yun-Pyo Hong, and Hong-Yeop Song

Yonsei University

Seoul, Korea

Outline

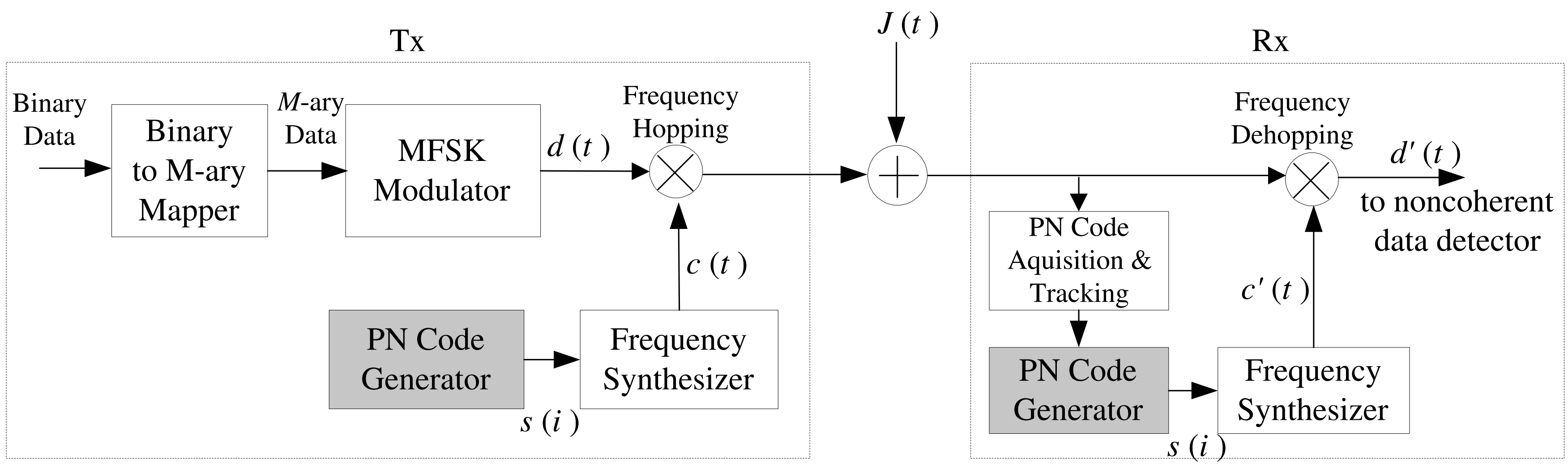
- Motives
- FH Systems
- *Strictly-Optimal* FH Sequences
- Summary & Remarks

Motives

- Most of FH sequences so far have been designed so that
  - their maximum periodic Hamming correlation is minimized
  - with the number of hopping slots (frequencies) that is a power of a prime.

- Usually, the correlation window is shorter than the period of the FH sequence.
  $\Rightarrow$ A sequence having good partial Hamming autocorrelation ?

Tx & Rx structure of a FH system



- Correlation window length
  - usually shorter than the period of the FH sequence due to the limited synchronization time or hardware complexity
  - may vary depending on the channel condition

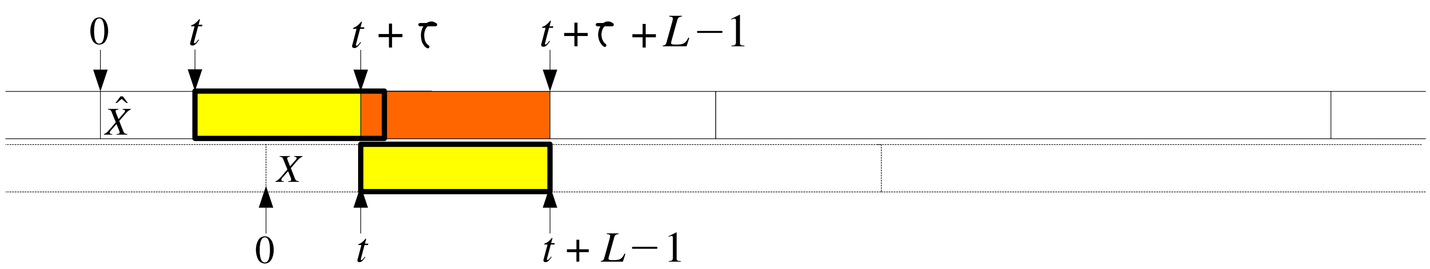
FH sequences with optimal partial autocorrelation properties

◇ Optimal criteria on partial Hamming autocorrelation

- Partial Hamming correlation function for a period N and a correlation window length L starting at t,

$$H_{XY}(\tau; t \mid L) = \sum_{j=t}^{t+L-1} h[x(j), y(j+\tau)],\ 0 \leq \tau < N \tag{1}$$

where $h[x,y] = 1$ if $x = y$ and $h[x,y] = 0$ if $x \neq y$.



- The maximum of the partial Hamming autocorrelation function (p-HAF)

$$H(X \mid L) = \max_{0<\tau<N,\ 0\leq t<N} \{H_{XX}(\tau; t \mid L)\}. \tag{2}$$

◇ Optimal criteria

- Let Ω be the set of all sequences of length N over a given alphabet A. We can state that a sequence $X(\in \Omega)$ is *strictly-optimal* if

$$H(X \mid L) \leq H(X' \mid L) \tag{3}$$

for all $L \leq N$ and all $X' \in \Omega$.

- What is the lower bound of $H(X \mid L)$?

- **Lemma 1 (Lempel'74)** *For every sequence* $X = \{x(j)\}$ *of period* N *over an alphabet* A *of size* $|A| = m$,

$$\begin{aligned} H(X) &\geq \overline{H}(X) \\ &= \frac{1}{N-1} \sum_{\tau=1}^{N-1} H_{XX}(\tau) \\ &\geq \frac{(N-b)(N+b-m)}{m(N-1)} \end{aligned} \tag{4}$$

where $b \ (0 \leq b < N) \equiv N \pmod q$ *and* $H_{XX}(\tau) = H_{XX}(\tau; 0 \mid N)$

- **Corollary 1**

$$\begin{aligned} H(X\,|L\,) &\geq \overline{H}(X \mid L) \\ &= \frac{\sum_{\tau=1}^{N-1} \sum_{t=0}^{N-1} H_{XX}(\tau; t \mid L)}{(N-1)N} \\ &= \frac{L}{N}\, \overline{H}(X) \\ &\geq \frac{L}{N}\, \frac{(N-b)(N+b-m)}{m(N-1)} \end{aligned} \tag{5}$$

◇ Generalized *m*- and GMW sequences

- A polynomial residue class ring: $R = GF(p)[\xi]/(w(\xi)^k)$
  where $w(\xi)$ = an irreducible polynomial of degree m over $GF(p)$, $m \geq 1$.

- In this paper, we only consider $m = 1$ particularly, $R = GF(p)[\xi]/(\xi^k)$.

- Any element $b \in R$, ideal basis representation:

$$b = b_0 + b_1\xi + \cdots + b_{k-1}\xi^{k-1}$$

  where $b_i \in GF(p)$. Thus, R can be written as

$$R = GF(p) + \xi GF(p) + \cdots + \xi^{k-1}GF(p).$$

- The Galois extension ring of R: $GR(R,r) = R[x]/(f(x))$

  where $f(x)$ is a basic monic irreducible polynomial of degree r over R.

  - choose $f(x)$ among monic irreducible polynomials over $GF(p)$.

- any element $\beta(\in GR(R,r))$ and $GR(R,r)$ can be expressed as

$$\begin{aligned}\beta =& \beta_0 + \beta_1\xi + \cdots + \beta_{k-1}\xi^{k-1},\\ GR(R,r) =& GF(p^r) + \xi GF(p^r) + \cdots + \xi^{k-1}GF(p^r)\end{aligned}$$

  where $\beta_i \in GF(p^r)$.

- If $s|r$, $\quad Tr_s^r(\cdot)$: $GR(R,r) \rightarrow GR(R,s)$

$$Tr_s^r(\beta) = \sum_{j=0}^{k-1} tr_s^r(\beta_j)\xi^j \tag{6}$$

  where $tr_s^r(v) = \sum_{i=0}^{(r/s)-1} v^{p^{si}}$ is the field trace function from $GF(p^r)$ to $GF(p^s)$.

- α = a root of a primitive basic irreducible polynomial $f(x)$ over $R = GF(p)[\xi]/(\xi^k)$

- A *GM* sequence over R [Udaya'98]:

$$s^{\nu}(i) = Tr_1^r(\nu\alpha^i), \qquad \nu \in GR(R,r).$$

- For $a = \sum_{i=0}^{k-1} a_i \xi^i \in GR(R,s)$, define a permutation monomial:

$$\Psi^d : a \mapsto \sum_{i=0}^{k-1} a_i^d \xi^i$$

  where $\gcd(d, p^s - 1) = 1$.

- GGMW sequence over R [Udaya'98]:

$$s^{\nu}(i) = Tr_1^s(\Psi^d[Tr_s^r(\nu\alpha^i)]), \quad \nu \in GR(R,r)$$

  where $s|r$.

- For any p^k-ary sequences, say X, of period $p^{2k}-1$,

$$H(X\,|L\,) \geq \left\lceil \frac{L}{p^k+1} \right\rceil. \tag{7}$$

- **Theorem 1** *Let* $f(x)$ *be a degree* $2k$ *primitive polynomial over* $GF(p)$, $f(\alpha)=0$ *and* $\gcd(d, p^k-1)=1$. *A GGMW sequence* $\{s^\nu(i)\}$,

$$s^\nu(i) = Tr_1^k\big(\Psi^d[Tr_k^{2k}(\nu\alpha^i)]\big), \quad \nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 + \cdots + \alpha^{e_{k-1}}\xi^{k-1} \in GR(R, 2k)$$

is strictly-optimal *if and only if* $\alpha^{e_0 d}$, $\alpha^{e_1 d}$, $\alpha^{e_2 d}$, $\ldots$, $\alpha^{e_{k-1} d}$ *are linearly independent over* $GF(p)$ *and*

$$e_i \equiv e_j \pmod{p^k+1}, \quad \forall\, i,\ j,\ \ 0 \leq i,j \leq k-1.$$

- **Corollary 2** *Let $f(x)$ be a degree $2k$ primitive polynomial over $GF(p)$ and $f(\alpha) = 0$. A GM sequence $\{s^{\nu}(i)\}$,*

$$s^{\nu}(i) = Tr_1^{2k}(\nu\alpha^i), \quad \nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 + \cdots + \alpha^{e_{k-1}}\xi^{k-1} \in GR(R, 2k)$$

is strictly-optimal *if and only if α^{e_0}, α^{e_1}, α^{e_2}, $\ldots$, $\alpha^{e_{k-1}}$ are linearly independent over $GF(p)$ and*

$$e_i \equiv e_j \pmod{p^k + 1}, \quad \forall\, i,\ j,\ 0 \le i, j \le k-1.$$

- For such p^k-ary *strictly-optimal* sequences of period $p^{2k} - 1$,

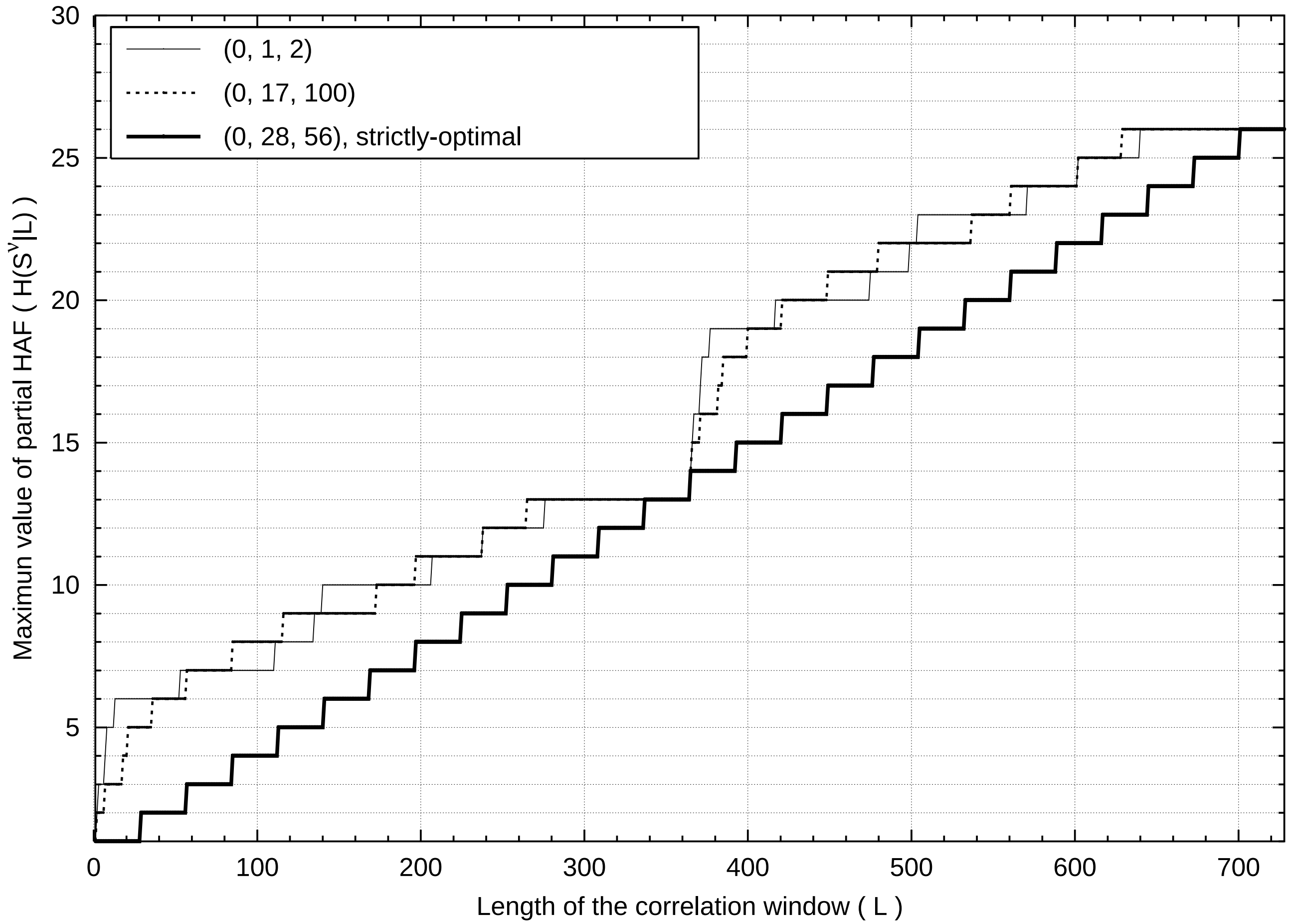
$$H(S^{\nu} \,|L\,) = \left\lceil \frac{L}{p^k + 1} \right\rceil. \tag{8}$$

◇ **Example 1** Three GM sequences over $R = GF(3)[\xi]/\xi^3$ where

$$s^{\nu}(i) = Tr_1^{6}(\nu\alpha^i), \quad \nu = \alpha^{e_0} + \alpha^{e_1}\xi + \alpha^{e_2}\xi^2 \in GR(R, 6)$$

and α is a root of a primitive polynomial $x^6 + x + 2$ over $GF(3)$.

(e_0, e_1, e_2)	GM Sequences (Frequency Hopping Patterns)
$(0, 1, 2)$	0 0 0 9 3 1 0 0 18 15 5 1 0 9 12 13 4 1 18 6 2 9 3 10 21 7 20 15 23 25 26 $\cdots$
$(0, 17, 100)$	21 0 9 15 18 19 21 18 3 24 2 7 3 24 15 25 4 4 15 9 20 21 0 25 6 19 8 21 14 19 17 $\cdots$
$(0, 28, 56)$	24 3 6 15 24 22 21 6 18 18 5 1 24 15 0 25 4 13 9 15 14 21 18 4 3 4 20 3 26 1 2 $\cdots$



Summary & Further Work

- FH sequences having optimal partial Hamming autocorrelation properties
  - Optimal criteria on partial Hamming autocorrelation
  - Classification of *Strictly-optimal* p^k-ary generalized *m*-sequences and generalized GMW sequences of period $p^{2k}-1$
  - Useful for synchronizing process

- We have only considered the case in which $R = GF(p)[\xi]/(\xi^k)$
  $\Rightarrow$ general description for deg($w(\xi)$)> 1