Frequency/Time Hopping Sequences with Large Linear Complexities

2005. 3. 15.

Yun-Pyo Hong and Hong-Yeop Song

Yonsei University

Seoul, Korea

Outline

- Motives
- Sequences over $GF(p^k)$ with Minimal Polynomials over $GF(p)$
- Frequency/Time Hopping Sequence Generators with Multiple LFSRs
- Concluding Remarks

Motives

◇ Frequency/time hopping (FH/TH) sequences

- Let L be the linear complexity (LC) of an FH/TH sequence. When the interceptor observes successive $2L$ frequency/time slots, he can successfully synthesize the next frequency/time slots using, say, Berlekamp-Massey (BM) algorithm

- Design non-binary sequences (for FH/TH sequences)

  (i) with "large" LC, and

  (ii) over "large" alphabet, but

  (iii) with "little" increase in the hardware complexity

- Non-binary sequences T from a given sequence S by simply reading its successive k-tuples

  $\Rightarrow$ Satisfies the above last two conditions, but How about LC?

Sequences over $GF(p^k)$ with Minimal Polynomials over $GF(p)$

◇ Preliminaries

- Given sequence $S = \{s_n | n = 0, 1, 2, ...\}$ over $GF(p)$
- New sequence (an FH/TH sequence) $T(k, S) = \{t_n | n = 0, 1, 2, ...\}$ over $GF(p)^k$:

$$t_n = (s_n, s_{n-1}, \ldots, s_{n-k+1}) \tag{1}$$

- Regard $T(k, S)$ being over the field $GF(p^k)$ using some but fixed basis

Proposition 1 *The LFSR that generates a sequence* $S = \{s_n\}$ *over* $GF(p)$ *also generates* $T(k, S)$ *over* $GF(p^k)$ *as defined in* (1) *regardless of the choice of basis. The converse holds provided that the characteristic polynomial that generates* T *over* $GF(p^k)$ *is essentially over* $GF(p)$.

◇ Issues for Proposition 1

- Proposition 1 does not guarantee that the LFSR for $T(k, S)$ over $GF(p^k)$ is necessarily the shortest possible even if it is the shortest for S over $GF(p)$, but that the LC of $T(k, S)$ is at most that of S
- Shortest LFSR for $T(k, S)$ over $GF(p^k)$ (and hence the LC of $T(k, S)$) cannot be uniquely determined unless a basis of $GF(p^k)$ is fixed

◇ **Question 1: Is it possible that the shortest LFSR that generates S over $GF(p)$ is indeed the shortest LFSR that generates $T(k, S)$ over $GF(p^k)$ with respect to any basis of $GF(p^k)$ over $GF(p)$?**

⇒ **Answer to the question: YES !**

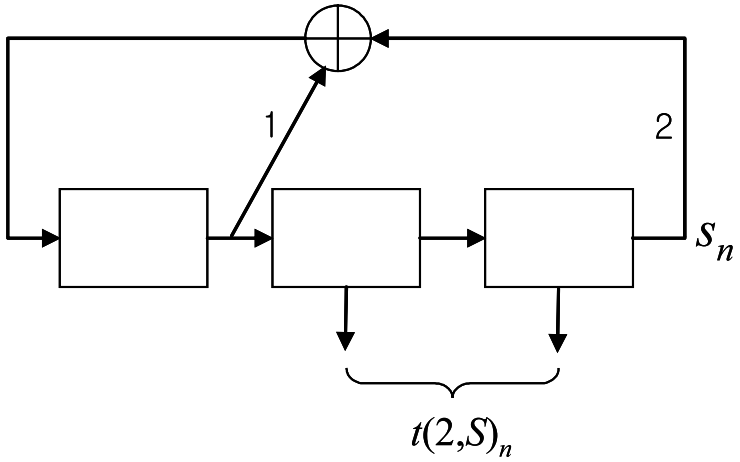
Theorem 2 *Let the minimal polynomial $C(x)$ of $S = \{s_n\}$ over $GF(p)$ be given by $C(x) = \prod_{i \in I}(f_i(x))^{m_i}$ for some irreducible polynomials $f_i(x)$ of degree d_i over $GF(p)$, some positive integers m_i, and some index set I. Let $T(k, S)$ over $GF(p^k)$ be defined as in* (1) *with respect to some but fixed basis for $k \geq 1$. Then, the minimal polynomial of $T(k, S)$ is the same as that of S and therefore, their LCs are same, if k and d_i are relatively prime for all $i \in I$.*

- Construct p^k-ary FH/TH sequences as in Theorem 2 whose LCs are the same as that of the original (that is the maximum possible) with respect to any basis from p-ary sequences

Application 3 *For a p-ary m-sequence S of period $p^r - 1$, the minimal polynomial of S is primitive polynomial of degree r. Therefore, the minimal polynomial of $T(k, S)$ over $GF(p^k)$ as defined in* (1) *is the same as that of S with respect to any basis if k is relatively prime to r.*

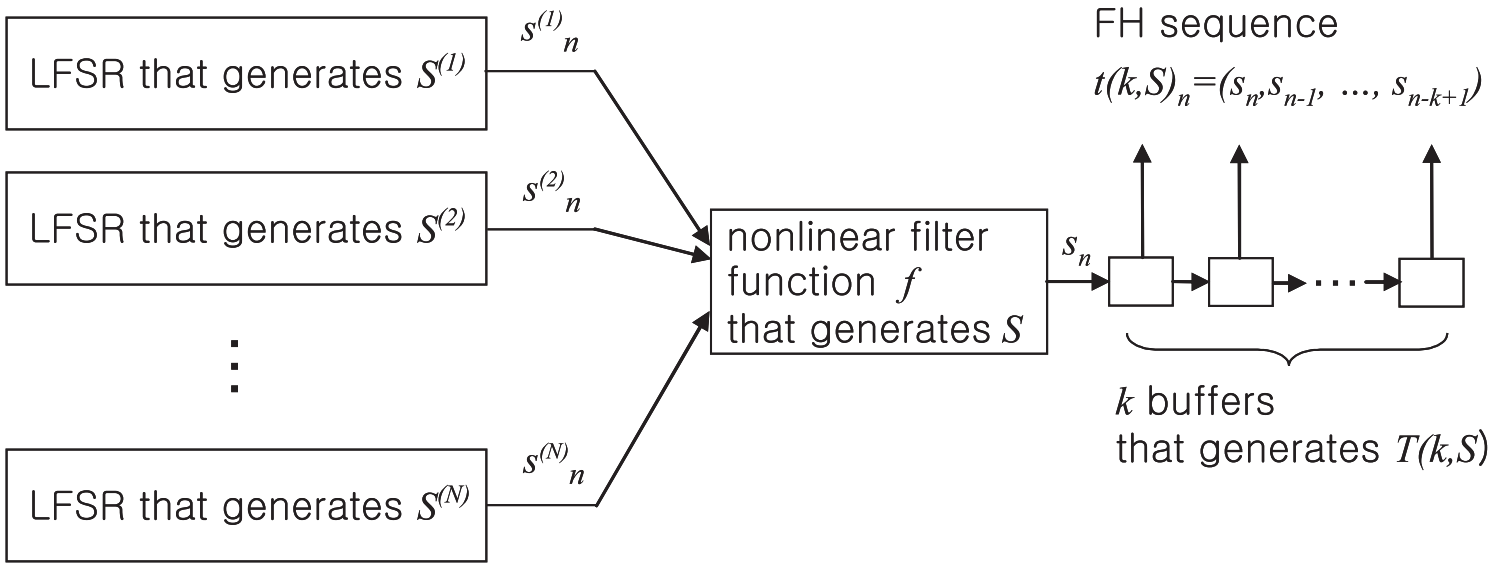
Application 4 *If a binary sequence S has a period 2^r (for example, binary de Bruijn sequences), then the minimal polynomial of S is of the form $(1 + x)^\tau$ for some positive integer τ. Therefore, the minimal polynomial of $T(k, S)$ over $GF(p^k)$ as defined in* (1) *is the same as that of S with respect to any basis for any positive integer k.*

◇ Example 1: A ternary m-sequence S of period $3^3 - 1$ and a 9-ary FH/TH sequence $T(2, S)$



- S : 0 0 1 1 1 0 2 1 1 2 1 0 1 0 0 2 2 2 0 1 2 2 1 2 0 2 ...
- $T(2, S)$: 02 00 10 11 11 01 20 12 11 21 12 01 10 01 00 20 22 22 02 10 21 22 12 21 02 20 ...
- Decimal version of $T(2, S)$: 2 0 3 4 4 1 6 5 4 7 5 1 3 1 0 6 8 8 2 3 7 8 5 7 2 6 ...
- S and $T(2, S)$ have the same minimal polynomial because $gcd(3, 2) = 1$

FH/TH Sequence Generators with Multiple LFSRs



- R. A. Rueppel ('86) characterized those LFSRs such that a nonlinearly filtered sequence, S, has the maximum possible LC given nonlinear filter function f.
- We characterized those p-ary sequences, S, whose k-tuple versions, $T(k, S)$, now over $GF(p^k)$ have the maximum possible LCs.
- Pay attention to the relations between the above two characterizations!

- $S^{(i)} = \{s_n^{(i)} | n = 0, 1, 2, ...\},\ i = 1, 2, \ldots, N$, are sequences over $GF(p)$

- Nonlinearly filtered sequence, S, over $GF(p)$ in algebraic normal form

$$s_n = f(s_n^{(1)}, s_n^{(2)}, \ldots, s_n^{(N)}) = a_0 + \sum_{i=1}^{N} a_i s_n^{(i)} + \sum_{i=1}^{N} \sum_{j=1}^{N} a_{ij} s_n^{(i)} s_n^{(j)} + \ldots + a_{12\ldots N} s_n^{(1)} s_n^{(2)} \ldots s_n^{(N)} \tag{2}$$

  - $f(\cdot)$ is a nonlinear filter function
  - $a_i,\ a_{ij},\ \ldots,\ a_{12\ldots N}$ and Operations are over $GF(p)$

- Maximum possible LC of the output sequence, S, given nonlinear filter function f

$$M = F(M^{(1)}, M^{(2)}, \ldots, M^{(N)}) \tag{3}$$

  - $M^{(i)}$ is the LC of $S^{(i)}$
  - $F(\cdot)$ is defined as $f(\cdot)$ in (2)
  - Operations are over the integers
  - a_i, a_{ij}, $\ldots$, $a_{12\ldots N}$ is 0 if a_i, a_{ij}, $\ldots$, $a_{12\ldots N}$ is 0 or 1 otherwise, respectively

◇ **Question 2: Is it possible to characterize those LFSRs such that both their nonlinearly filtered sequence, S, over $GF(p)$ has the maximum possible LC, M, and $T(k, S)$ over $GF(p^k)$ has the same minimal polynomials as that of S?**

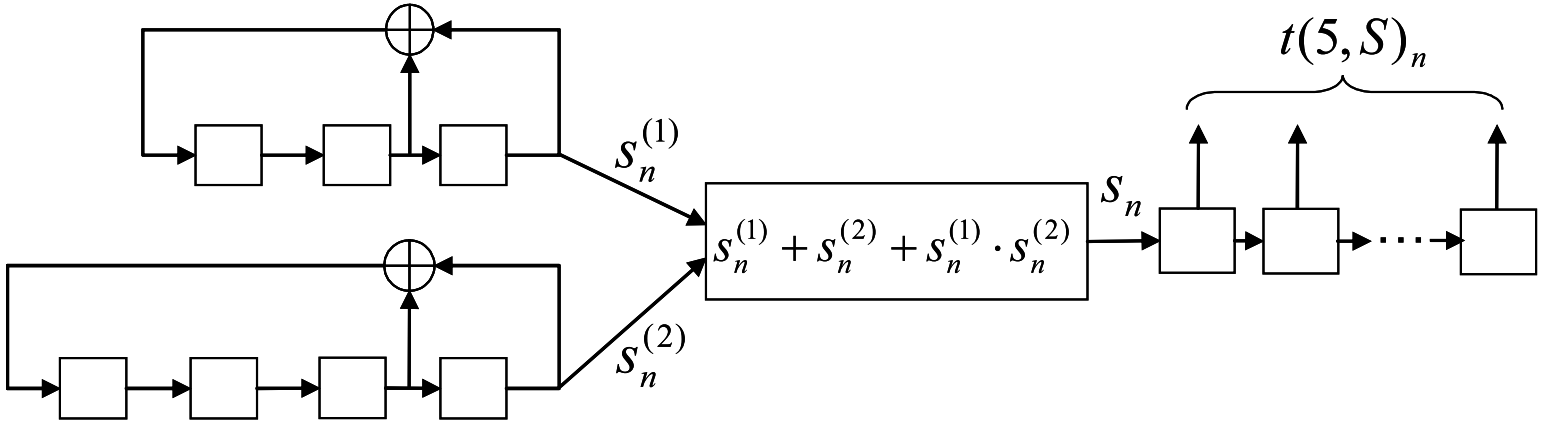
⇒ **Answer to the question: YES !**

Lemma 5 (Rueppel '86) *Let* $S^{(i)},\ i = 1, 2, \ldots, N$, *be sequences over* $GF(p)$ *with minimal polynomials* $C_{S^{(i)}}(x)$ *of degree* $M^{(i)}$, *that divide* $x^{p^{m^{(i)}}-1} - 1$ *for some* $m^{(i)}$ *and contain no linear factor. For any pair of distinct roots,* α *and* β, *of* $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, $\alpha\beta^{-1} \notin GF(p)$. *If* $m^{(i)},\ i = 1, 2, \ldots, N$ *are pairwise relatively prime, then* S *over* $GF(p)$ *as defined in* (2) *given nonlinear filter function* f *have the minimal polynomial of degree* M *as defined in* (3).

Corollary 6 *Let* S *be a sequence over* $GF(p)$ *as constructed in* Lemma 5. *If* $\prod_{i=1}^{N} m^{(i)}$ *and* k *are relatively prime, then* $T(k, S)$ *over* $GF(p^k)$ *as defined in* (1) *has the same minimal polynomial as that of* S.

- Construct p^k-ary FH/TH sequences as in Corollary 6 whose LCs are the maximum possible for a given nonlinear filter function

◇ Example 2: An FH/TH sequence generator



- S : 00111111010111101011111111111101110110111111011100111111111111
  01111101111110110111101111100101110111111 . . .
- Decimal version of $T(5, S)$: 15 7 19 25 28 30 31 31 15 23 11 21 26 29 30 15 . . .
- LC of S is 19 $(= 3 + 4 + 3 \cdot 4)$ (the maximum possible)
- $T(5, S)$ has the same minimal polynomial as that of S because $gcd(3 \times 4, 5) = 1$

Concluding Remarks

- We characterize those p-ary sequences whose k-tuple versions now over $GF(p^k)$ have the maximum possible LCs.

- We consider the FH/TH sequence generators composed of multiple LFSRs, one nonlinear filter function, and some buffers.

- We characterize the generators whose output FH/TH sequences over $GF(p^k)$ have the maximum possible LC for a given nonlinear filter function.