Perfect polyphase sequences from cubic polynomials

Min Kyu Song
Yonsei University

Supervisor: prof. Hong-Yeop Song

2017 Sino-Korea conference on coding theory and its related topics

July 10-15, 2017

NIMS, KOREA

Polyphase sequences

- Polyphase sequence (root-of-unity sequence)
  - All the terms in the sequence are on the complex unit circle.
  - Identified by its phase sequence, e.g.,

$$\left\{e^{-j2\pi\frac{1}{4}}, e^{-j2\pi\frac{2}{4}}, e^{-j2\pi\frac{0}{4}}, e^{-j2\pi\frac{2}{4}}\right\}$$

$$\Updownarrow$$

$$\{1, 2, 0, 2\}$$

4-ary polyphase sequence of period 4

Correlation

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two M-ary sequences of length L, then (periodic) correlation between x and y at time shift τ is

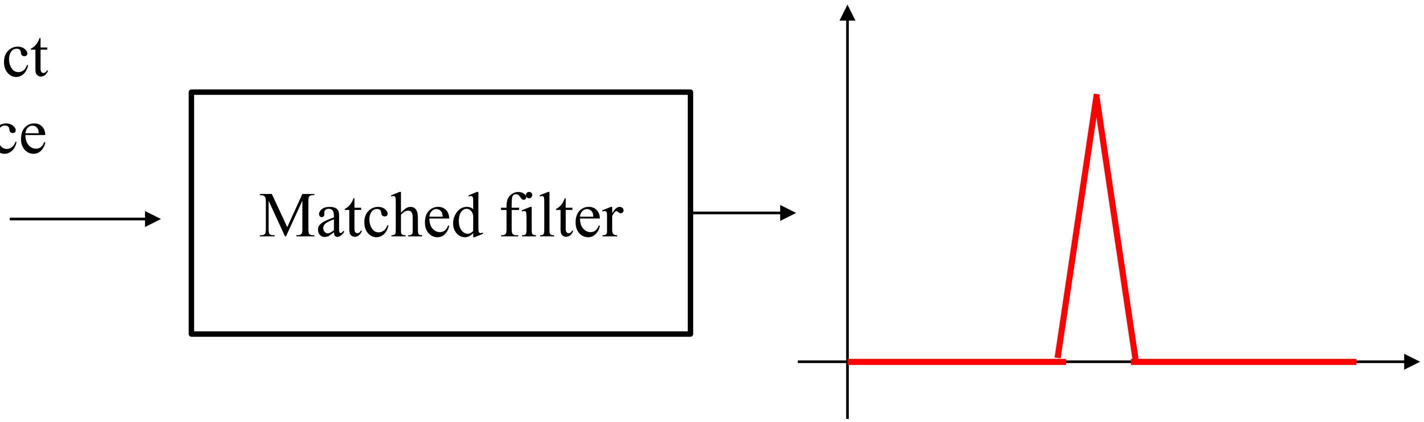
$$\mathrm{C}_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \omega_M^{y(n+\tau)-x(n)}$$

where $\omega_M = e^{-\frac{j2\pi}{M}}$.

- A sequence is referred to a **perfect sequence** if its autocorrelation is zero for any time shift $\tau \not\equiv 0 \ (mod\ L)$.

Use in communication systems

A perfect sequence

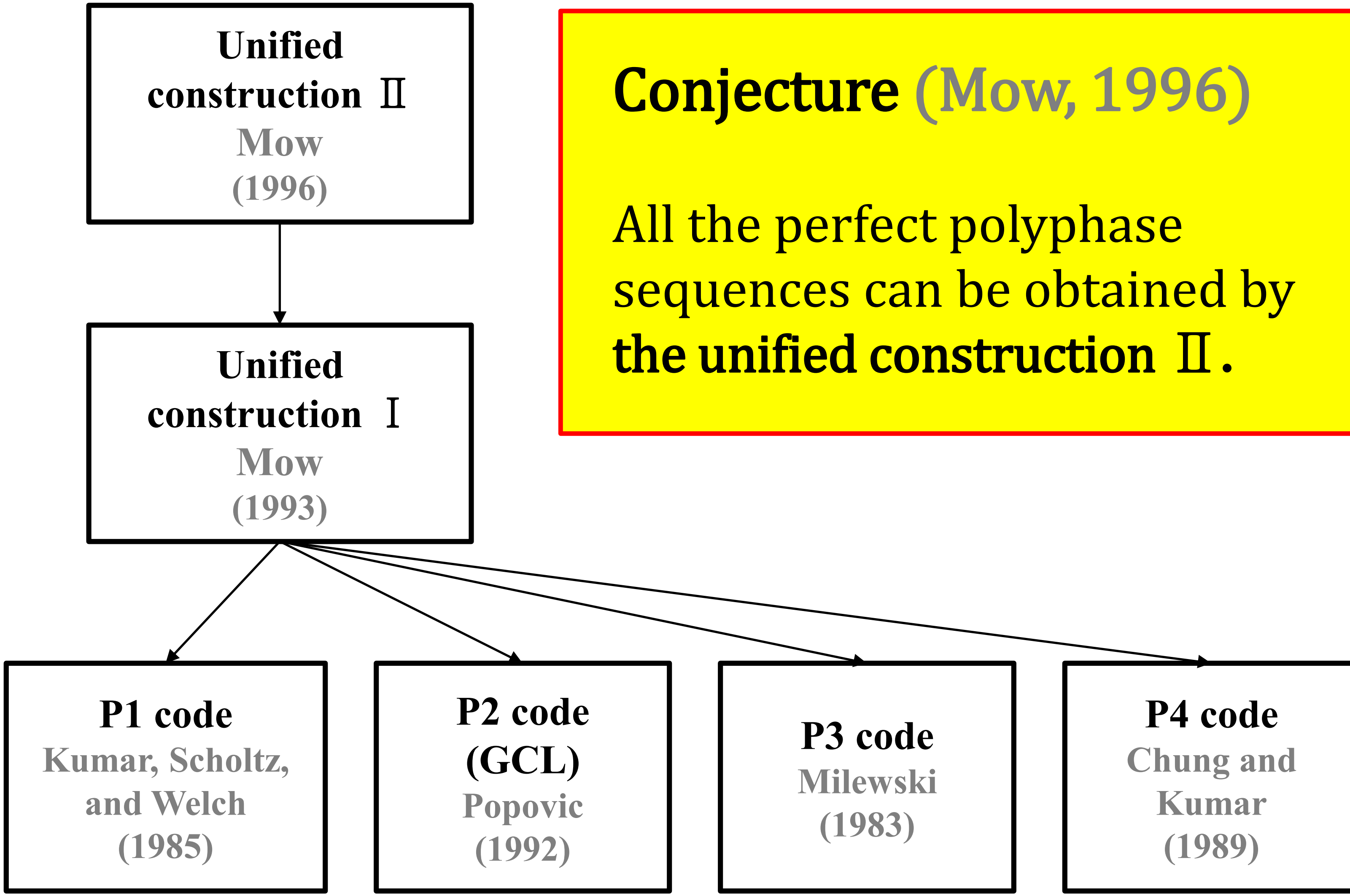


Impulse-like output
(Noise free)

Applications

- *Ranging*
- *Synchronization*
- *DS-CDMA*
- *etc.*

Current state



Conjecture (Mow, 1996)

All the perfect polyphase sequences can be obtained by **the unified construction Ⅱ.**

Goal

- For an odd prime p, we will consider a polyphase sequence

$$\boldsymbol{f} = \{f(n)\}_{n=0}^{p^k-1}$$

where

$$f(n) = an^3 + bn^2 + cn + d$$

is a cubic polynomial with coefficients $a, b, c,$ and d.
  - We may let $d = 0$ since it does not affect autocorrelation.

- Our objectives
  1. **When** the sequence $\boldsymbol{f}$ **becomes perfect**.
  2. **Relationship with** a well-known class of perfect polyphase sequences, called **Generalized Chirp-like (GCL) sequences**.

For the case of $a \equiv 0 \pmod{p^k}$

- A p^k-ary Zadoff-Chu sequence of period p^k is defined by

$$\boldsymbol{z} = \left\{ z(n) = \frac{un(n+1)}{2} + qn \ \left(mod\ p^k \right) \right\}_{n=0}^{p^k-1}$$

where $u \not\equiv 0 \pmod{p}$ and q is a integer.

- Proposition. If $a \equiv 0 \left(mod\ p^k \right), b \not\equiv 0\ (mod\ p)$, then $\boldsymbol{f} = \{f(n)\}_{n=0}^{p^k-1}$ with

$$f(n) = an^3 + bn^2 + cn$$

becomes a p^k-ary Zadoff-Chu sequence of period p^k with parameters $u = 2b$ and $q = c - 2b$

- In this case, $f(n)$ is actually of degree 2.

For the case of $a \not\equiv 0 \pmod{p^k}$

- Theorem. Let $\boldsymbol{f} = \{f(n)\}_{n=0}^{p^k-1}$ with

$$f(n) = an^3 + bn^2 + cn.$$

  1) Let $p = 3$. If $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, then the sequence $\boldsymbol{f}$ is a perfect sequence of period p^k.
  2) Let $p \geq 5$. If $a \not\equiv 0 \pmod{p^k}$, $b \not\equiv 0 \pmod{p}$, and $a \equiv 0 \pmod{p}$, then the sequence $\boldsymbol{f}$ is a perfect sequence of period p^k.

- In other choice of a, b, and c, $\boldsymbol{f}$ is not perfect.
  - There exists non-zero τ at which $C_{\boldsymbol{f}}(\tau) = \sqrt{\gcd(3a\tau, p^k)\, p^k}$.

A proof

- Assume that $p \geq 5, a \not\equiv 0 \left(\mathrm{mod}\ p^k\right)$, and $b \not\equiv 0 \ (\mathrm{mod}\ p), a \equiv 0 \ (\mathrm{mod}\ p)$. Observe that

$$\begin{aligned} & f(n+\tau) - f(n) \\ & \quad \equiv a(n+\tau)^3 + b(n+\tau)^2 + c(n+\tau) - [an^3 + bn^2 + cn] \\ & \quad \equiv 3a\tau n^2 + (3a\tau^2 + 2b\tau)n + \underbrace{\alpha}_{\text{some constant}} \pmod{p^k} \end{aligned}$$

Focus on the part `$3a\tau n^2 + (3a\tau^2 + 2b\tau)n \pmod{p^k}$'.

$$\begin{aligned} & 3a\tau n^2 + (3a\tau^2 + 2b\tau)n \pmod{p^k} \\ \leftrightarrow \ & \underbrace{3a}_{\equiv 0 \ (\mathrm{mod}\ p)}n^2 + (\underbrace{3a\tau + 2b}_{\not\equiv 0 \ (\mathrm{mod}\ p)})n \pmod{\gamma} \end{aligned} \qquad \gamma = \frac{p^k}{\gcd(\tau, p^k)}$$

That is a quadratic permutation polynomial over the integers modulo $\frac{p^k}{\gcd(3\tau, p^k)}$

A proof (cont')

- The autocorrelation of $\boldsymbol{f}$ at time shift $\tau \not\equiv 0 \pmod{p^k}$ is

$$\mathrm{C}_{\boldsymbol{f}}(\tau) = \sum_{n=0}^{L-1} \omega_M^{f(n+\tau)-f(n)}$$

$$= \omega_{p^k}^{\alpha} \sum_{n=0}^{L-1} \omega_{p^k}^{3a\tau n^2+\left(3a\tau^2+2b\tau\right)n}$$

$$= \omega_{p^k}^{\alpha} \sum_{n=0}^{L-1} \omega_{\gamma}^{3an^2+(3a\tau+2b)n} \qquad \gamma = \frac{p^k}{\gcd(3\tau, p^k)}$$

$$= \frac{p^k}{\gamma} \omega_{p^k}^{\alpha} \sum_{n=0}^{\gamma-1} \omega_{\gamma}^{3an^2+(3a\tau+2b)n}$$

$$= \frac{p^k}{\gamma} \omega_{p^k}^{\alpha} \boxed{\sum_{n\in Z_\gamma} \omega_{\gamma}^{\sigma(n)}} = 0$$

Is that new?

- To show whether it is new or not, we need to compare it with previous known perfect polyphase sequences.
- For the first step toward that, we compare it with Generalized Chirp-like (GCL) sequences due to Popovic in 1992.
- Our result is that

Some of them are not GCL sequences.

A viewpoint
– Extension of a ZC sequence

- The cubic polynomial $f(n)$ can be written as

$$f(n) \equiv an^3 + bn^2 + cn$$
$$\equiv s(n) + z(n) \pmod{p^k}$$

where

$$\boldsymbol{z} = \{z(n) = bn^2 + cn\}_{n=0}^{p^k-1}$$

is the Zadoff-Chu sequence in the previous proposition since $b \not\equiv 0 \pmod{p}$, and

$$\boldsymbol{s} = \{s(n) = an^3\}_{n=0}^{p^k-1}.$$

- Therefore, we can view the sequence $\boldsymbol{f}$ as a result of adding $\boldsymbol{s}$ to the Zadoff-Chu sequence $\boldsymbol{z}$ element-wise.

Previous extension of a ZC sequence

- The Generalized chirp-like (GCL) sequence is a well-known extension of the Zadoff-Chu sequence.

- Let u, v are positive integers with $p^k = uv^2$.

- A p^k-ary GCL sequence $\boldsymbol{g} = \{g(n)\}_{n=0}^{p^k-1}$ of period p^k is the result of adding $\boldsymbol{m}$ to $\boldsymbol{z}$
  - $\boldsymbol{z}$ is a p^k-ary Zadoff-Chu sequence of period p^k.
  - $\boldsymbol{m}$ is arbitrarily chosen sequence of length v.

- Obviously,

$$\boldsymbol{v \leq p^{\lfloor k/2 \rfloor}}.$$

How to compare – array form

p^k-ary Zadoff-Chu sequence $\boldsymbol{z}$ of period p^k

A period of $\boldsymbol{s}$

$\boldsymbol{s}$ +
$\boldsymbol{s}$ +
$\vdots$
$\boldsymbol{s}$ +

$\frac{p^k}{L} \times L$ array

$$L \overset{?}{\gtreqless} v$$

$\frac{p^k}{v} \times v$ array

A period of $\boldsymbol{m}$

\+ $\boldsymbol{m}$
\+ $\boldsymbol{m}$
$\vdots$
\+ $\boldsymbol{m}$

The perfect sequence $\boldsymbol{f}$ from cubic polynomial

The GCL sequence $\boldsymbol{g}$

Period of $\{an^3\}_{n=0}^{p^k-1}$

- Lemma. Let L be the period of the sequence

$$\boldsymbol{s} = \{s(n) = an^3\}_{n=0}^{p^k-1}$$

with $a \not\equiv 0 \pmod{p^k}$. Then,

$$L = \max\left(p^{\lceil k/3 \rceil}, \frac{p^k}{\gcd(3a, p^k)}\right).$$

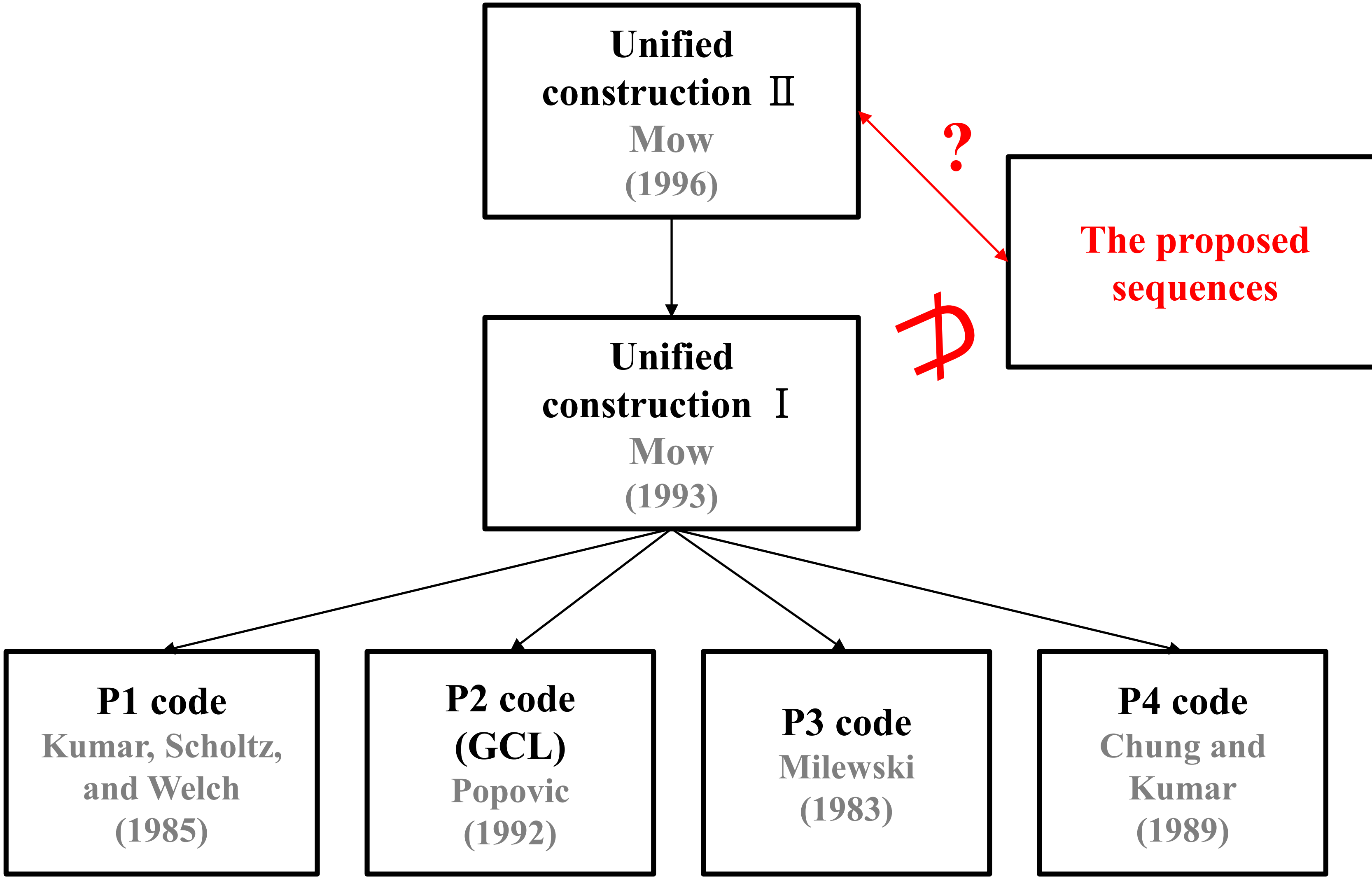
Comparison result

- Theorem. Consider the perfect sequence $\boldsymbol{f} = \{f(n)\}_{n=0}^{p^k-1}$ from the cubic polynomial $f(n)$.
  - Let $p = 3$ and write $a = 3^i t$ where t, i are some integers with $\gcd(t, 3) = 1$ and $0 \le i \le k-1$. If $k \ge 3$ and
  $$0 \le i < k - \left\lfloor \frac{k}{2} \right\rfloor - 1,$$
  then, the sequence $\boldsymbol{f}$ is not a GCL sequence.
  - Let $p \ge 5$ and write $a = p^i t$ where t, i are some integers with $\gcd(t, p) = 1$ and $0 \le i \le k$. If $k \ge 4$ and
  $$1 \le i < k - \left\lfloor \frac{k}{2} \right\rfloor,$$
  then, the sequence $\boldsymbol{f}$ is not a GCL sequence.

Some interesting questions

1. Are they modulatable like GCL?
2. What is the crosscorrelation among them?
   - How can we construct optimal set of perfect sequence families from them?
3. Compare them with all the other known perfect sequences.

Is that really new?



Any question or comment?