A generalized Milewski construction for perfect sequences

with PSK+/APSK+ constellations

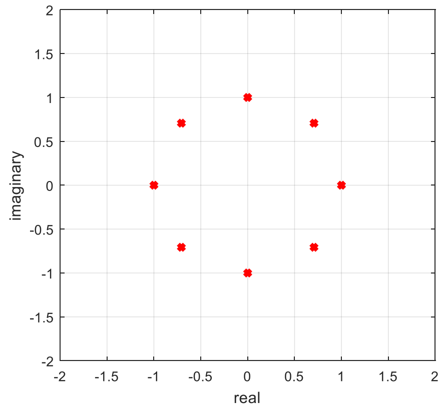
Min Kyu Song and Hong-Yeop Song

Yonsei University

SETA 2018, October 1-6

Constellations (alphabets)

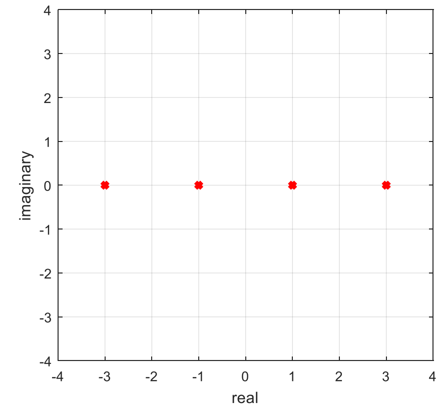
Phase shift keying (PSK) → **polyphase**



Phase only

well studied

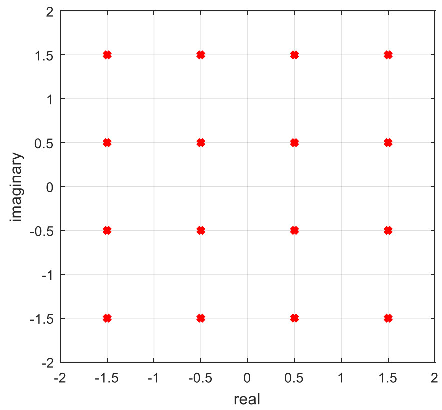
Amplitude shift keying (ASK)



real amplitude only

few results

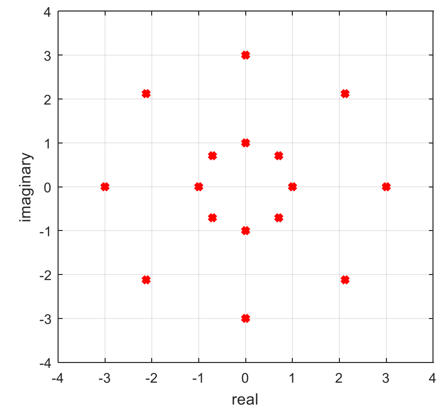
Quadrature-amplitude modulation (QAM)



Normally square

studied

Amplitude & phase shift keying (APSK)



Both Phase and Amplitude

few results

Adding the zero point ⇒ PSK+, ASK+, QAM+, and APSK+

Autocorrelation & perfect sequence

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ be a complex-valued sequence of length L.

  The (periodic) autocorrelation of $\boldsymbol{x}$ at time shift τ is

$$\mathrm{C}_{\boldsymbol{x}}(\tau) = \sum_{n=0}^{L-1} x(n)x^*(n-\tau) .$$

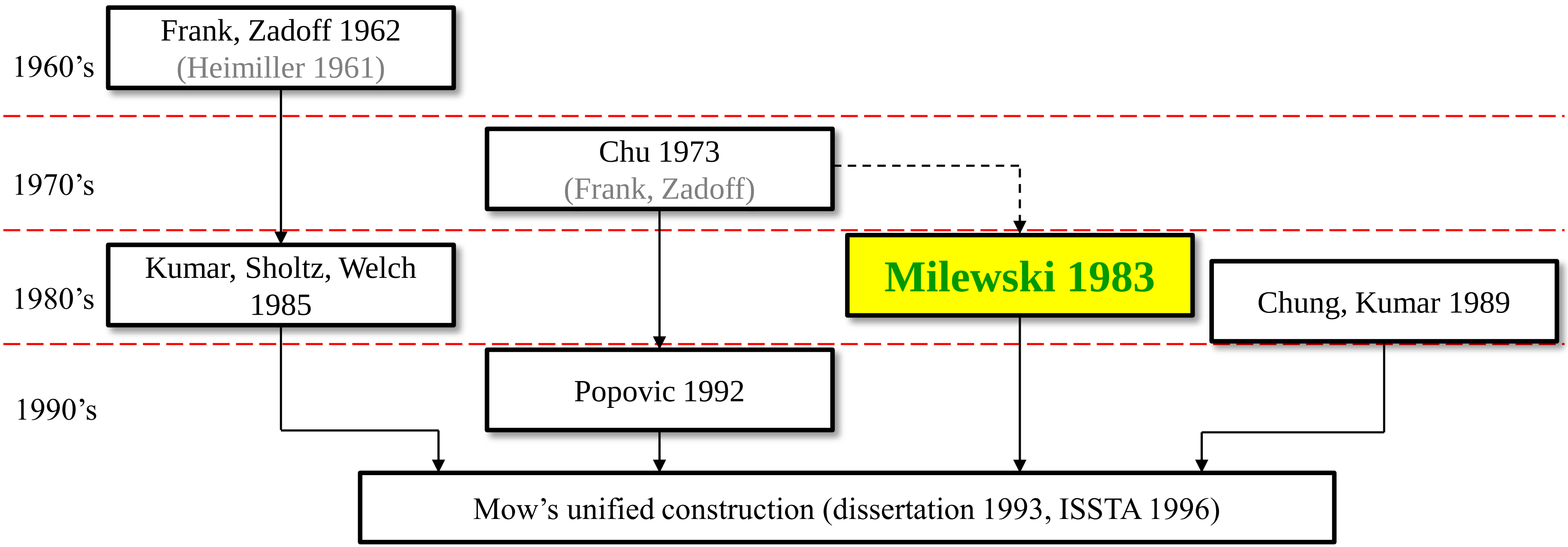
  - A sequence is perfect if its autocorrelation is zero for any $\tau \not\equiv 0 \pmod{L}$.

- x is a **perfect** sequence of period L **if and only if**

  the **DFT** of x has **flat magnitude**.

The Milewski construction

- Originally proposed to construct perfect **polyphase** sequences from those of shorter period
  - Well-known case: using the Zadoff-Chu sequence as the shorter one



The original construction

period: $m^1 \rightarrow m^{2K+1}$

perfect polyphase sequence

$\boldsymbol{\alpha} = \{\alpha(n)\}_{n=0}^{m-1}$

A positive integer

K

Milewski Construction

Output **perfect polyphase** sequence

$\boldsymbol{s} = \{s(n)\}_{n=0}^{\boldsymbol{m}^{2K+1}-1}$

where

$$s(n) = \alpha(q)\omega^{qr}$$

where $n = q\boldsymbol{m}^{\boldsymbol{K}} + r$.

and ω is an m^{K+1}-th complex primitive root of unity

The original construction

period: $m^1 \rightarrow m^{1+2K}$

perfect polyphase sequence

A positive integer

$\boldsymbol{\alpha} = \{\alpha(n)\}_{n=0}^{m-1}$ $\quad K$

Milewski Construction

Output perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{\boldsymbol{m}^{2K+1}-1}$$

where

$$s(n) = \alpha(q)\omega^{qr}$$

where $n = q\boldsymbol{m}^{K} + r$.

and ω is an m^{K+1}-th complex primitive root of unity

$m \cdot m^K \times m^K$ array form of $\boldsymbol{s}$

Input sequence of period m

$$\begin{pmatrix}
\alpha(0) \times \mathbf{1} & \alpha(0) \times \mathbf{1} & \cdots & \alpha(0) \times \mathbf{1} \\
\alpha(1) \times \mathbf{1} & \alpha(1) \times \boldsymbol{\omega} & \cdots & \alpha(1) \times \boldsymbol{\omega}^{m^K-1} \\
\alpha(2) \times \mathbf{1} & \alpha(2) \times \boldsymbol{\omega}^2 & \cdots & \alpha(2) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times \mathbf{1} & \alpha(m-1) \times \boldsymbol{\omega}^{m-1} & \cdots & \alpha(m-1) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) \times \mathbf{1} & \alpha(0) \times \boldsymbol{\omega}^{m^K} & \cdots & \alpha(0) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^{m^K} \\
\alpha(1) \times \mathbf{1} & \alpha(1) \times \boldsymbol{\omega}^{m^K+1} & \cdots & \alpha(1) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^{m^K+1} \\
\alpha(2) \times \mathbf{1} & \alpha(2) \times \boldsymbol{\omega}^{m^K+2} & \cdots & \alpha(2) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^{m^K+2} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times \mathbf{1} & \alpha(m-1) \times \boldsymbol{\omega}^{m^{K+1}-1} & \cdots & \alpha(m-1) \times \left(\boldsymbol{\omega}^{m^K-1}\right)^{m^{K+1}-1}
\end{pmatrix}$$

Our generalization

perfect polyphase sequence

$\boldsymbol{\alpha} = \{\alpha(n)\}_{n=0}^{m-1}$

A positive integer

K

Milewski Construction

Output
perfect polyphase sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{m^{2K+1}-1}$$

where

$$s(n) = \alpha(q)\omega^{qr}$$

with $n = q\boldsymbol{m^K} + r$, and

ω is an mN-th primitive root of unity with $N = m^K$.

Perfect sequence
not necessarily polyphase

$\boldsymbol{\alpha} = \{\alpha(n)\}_{n=0}^{m-1}$

A positive integer

N

not necessarily perfect
Any polyphase sequence of length N

$\boldsymbol{\mu}$

Generalized Milewski Construction

Output
perfect sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{mN^2-1}$$

where

$$s(n) = \mu(r)\alpha(q)\omega^{qr}$$

with $n = q\boldsymbol{N} + r$, and

ω is an mN-th primitive root of unity with any positive integer N.

Array Form

Assume that $\boldsymbol{\mu}$ is the all-1 sequence,

Column index $r = 0, 1, 2, \dots, N-1$

Row index $q = 0,1,2,\dots,mN-1$

$$
\begin{array}{llll}
\alpha(0) \times (\omega^{0})^{0} & \alpha(0) \times (\omega^{1})^{0} & \cdots & \alpha(0) \times (\omega^{N-1})^{0} \\
\alpha(1) \times (\omega^{0})^{1} & \alpha(1) \times (\omega^{1})^{1} & \cdots & \alpha(1) \times (\omega^{N-1})^{1} \\
\alpha(2) \times (\omega^{0})^{2} & \alpha(2) \times (\omega^{1})^{2} & \cdots & \alpha(2) \times (\omega^{N-1})^{2} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^{0})^{m-1} & \alpha(m-1) \times (\omega^{1})^{m-1} & \cdots & \alpha(m-1) \times (\omega^{N-1})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) \times (\omega^{0})^{m(N-1)} & \alpha(0) \times (\omega^{1})^{m(N-1)} & \cdots & \alpha(0) \times (\omega^{N-1})^{m(N-1)} \\
\alpha(1) \times (\omega^{0})^{m(N-1)+1} & \alpha(1) \times (\omega^{1})^{m(N-1)+1} & \cdots & \alpha(1) \times (\omega^{N-1})^{m(N-1)+1} \\
\alpha(2) \times (\omega^{0})^{m(N-1)+2} & \alpha(2) \times (\omega^{1})^{m(N-1)+2} & \cdots & \alpha(2) \times (\omega^{N-1})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^{0})^{mN-1} & \alpha(m-1) \times (\omega^{1})^{mN-1} & \cdots & \alpha(m-1) \times (\omega^{N-1})^{mN-1}
\end{array}
$$

※ ω is an mN-th primitive root of unity

Proof when $\boldsymbol{\mu}$ is all-1 sequence

$$\begin{pmatrix}
\alpha(0) \times (\omega^0)^0 & \alpha(0) \times (\omega^1)^0 & \cdots & \alpha(0) \times (\omega^{N-1})^0 \\
\alpha(1) \times (\omega^0)^1 & \alpha(1) \times (\omega^1)^1 & \cdots & \alpha(1) \times (\omega^{N-1})^1 \\
\alpha(2) \times (\omega^0)^2 & \alpha(2) \times (\omega^1)^2 & \cdots & \alpha(2) \times (\omega^{N-1})^2 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^0)^{m-1} & \alpha(m-1) \times (\omega^1)^{m-1} & \cdots & \alpha(m-1) \times (\omega^{N-1})^{m-1} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) \times (\omega^0)^{m(N-1)} & \alpha(0) \times (\omega^1)^{m(N-1)} & \cdots & \alpha(0) \times (\omega^{N-1})^{m(N-1)} \\
\alpha(1) \times (\omega^0)^{m(N-1)+1} & \alpha(1) \times (\omega^1)^{m(N-1)+1} & \cdots & \alpha(1) \times (\omega^{N-1})^{m(N-1)+1} \\
\alpha(2) \times (\omega^0)^{m(N-1)+2} & \alpha(2) \times (\omega^1)^{m(N-1)+2} & \cdots & \alpha(2) \times (\omega^{N-1})^{m(N-1)+2} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^0)^{mN-1} & \alpha(m-1) \times (\omega^1)^{mN-1} & \cdots & \alpha(m-1) \times (\omega^{N-1})^{mN-1}
\end{pmatrix} \triangleq (\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1})$$

where

$$\boldsymbol{s}_r = \{s_r(q) = \alpha(q)(\omega^r)^q\}_{q=0}^{mN-1}$$

is the r-th column

We will use linearity of the DFT.

Proof - continued

$$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1}) = \underline{(\boldsymbol{s}_0, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})} + \cdots + (\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \boldsymbol{s}_{N-1})$$

$$\begin{pmatrix}
\alpha(0) \times (\omega^{0})^{\mathbf{0}} & 0 & \cdots & 0 \\
\alpha(1) \times (\omega^{0})^{\mathbf{1}} & 0 & \cdots & 0 \\
\alpha(2) \times (\omega^{0})^{\mathbf{2}} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^{0})^{\boldsymbol{m-1}} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) \times (\omega^{0})^{\boldsymbol{m(N-1)}} & 0 & \cdots & 0 \\
\alpha(1) \times (\omega^{0})^{\boldsymbol{m(N-1)+1}} & 0 & \cdots & 0 \\
\alpha(2) \times (\omega^{0})^{\boldsymbol{m(N-1)+2}} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) \times (\omega^{0})^{\boldsymbol{mN-1}} & 0 & \cdots & 0
\end{pmatrix}$$

Proof - continued

$$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1}) = \underline{(\boldsymbol{s}_0, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})} + \cdots + (\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \boldsymbol{s}_{N-1})$$

$$\begin{pmatrix}
\alpha(0) & 0 & \cdots & 0 \\
\alpha(1) & 0 & \cdots & 0 \\
\alpha(2) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) & 0 & \cdots & 0 \\
\alpha(1) & 0 & \cdots & 0 \\
\alpha(2) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) & 0 & \cdots & 0
\end{pmatrix}$$

Proof - continued

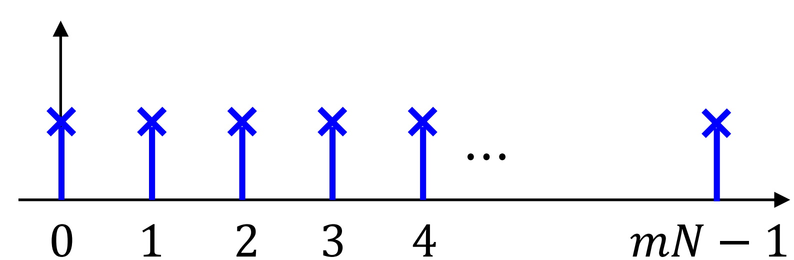
$$(s_0, s_1, s_2, \dots, s_{N-1}) = (s_0, 0, 0, \dots, 0) + \cdots + (0, 0, \dots, 0, s_{N-1})$$

$$\begin{pmatrix}
\alpha(0) & 0 & \cdots & 0 \\
\alpha(1) & 0 & \cdots & 0 \\
\alpha(2) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(0) & 0 & \cdots & 0 \\
\alpha(1) & 0 & \cdots & 0 \\
\alpha(2) & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
\alpha(m-1) & 0 & \cdots & 0
\end{pmatrix}$$

A perfect sequence of period mN

repeat N times

Its DFT has flat magnitude

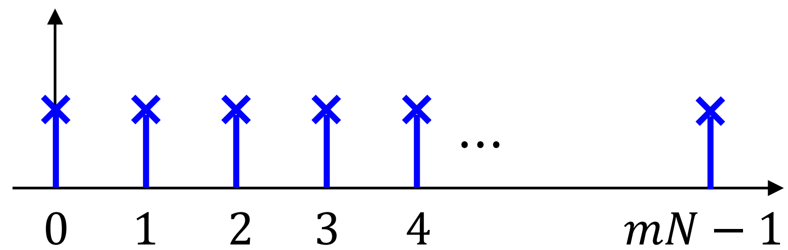


Proof - continued

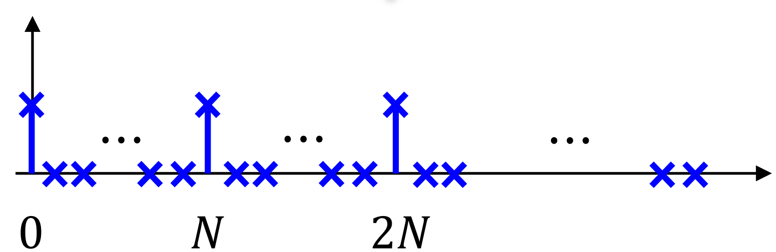
$$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1}) = \underline{(\boldsymbol{s}_0, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})} + \cdots + (\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \boldsymbol{s}_{N-1})$$

$$\begin{pmatrix} \alpha(0) & 0 & \cdots & 0 \\ \alpha(1) & 0 & \cdots & 0 \\ \alpha(2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(m-1) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(0) & 0 & \cdots & 0 \\ \alpha(1) & 0 & \cdots & 0 \\ \alpha(2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(m-1) & 0 & \cdots & 0 \end{pmatrix}$$

DFT has flat magnitude



repeat
N times

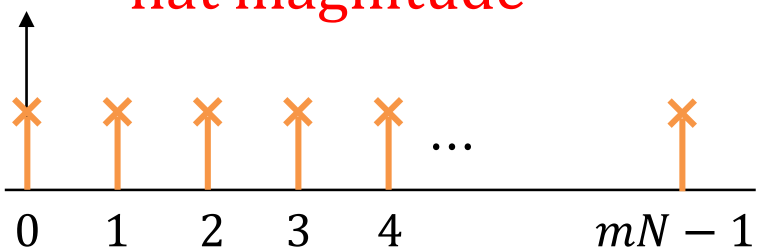


Proof - continued

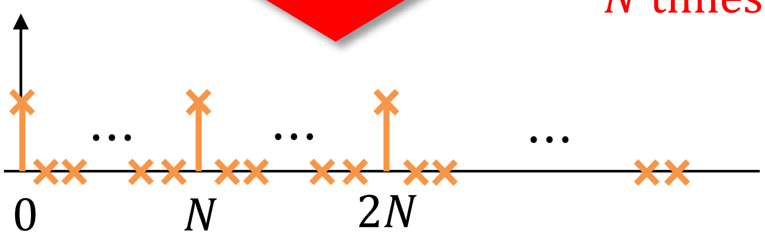
$(\mathbf{0}, \boldsymbol{s_1}, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})$: 1-cyclic shift of $\underline{(\boldsymbol{s_1}, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})}$

Cyclic shift at time domain does not affect on magnitude at the frequency domain

DFT has flat magnitude

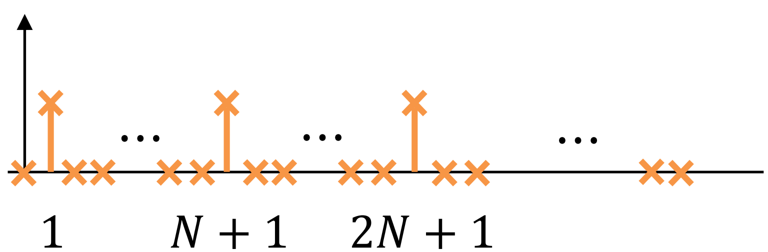


repeat N times



$$
\begin{pmatrix}
\boxed{\begin{matrix} \alpha(0) & 0 & \cdots & 0 \\ \alpha(1) & 0 & \cdots & 0 \\ \alpha(2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(m-1) & 0 & \cdots & 0 \end{matrix}} \\
\begin{matrix} \vdots & \vdots & \ddots & \vdots \\ \alpha(0) & 0 & \cdots & 0 \\ \alpha(1) & 0 & \cdots & 0 \\ \alpha(2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(m-1) & 0 & \cdots & 0 \end{matrix}
\end{pmatrix}
\otimes
\begin{pmatrix}
(\omega^1)^0 & 0 & \cdots & 0 \\
(\omega^1)^1 & 0 & \cdots & 0 \\
(\omega^1)^2 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
(\omega^1)^{m-1} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
(\omega^1)^{m(N-1)} & 0 & \cdots & 0 \\
(\omega^1)^{m(N-1)+1} & 0 & \cdots & 0 \\
(\omega^1)^{m(N-1)+2} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
(\omega^1)^{mN-1} & 0 & \cdots & 0
\end{pmatrix}
$$

1-cyclic shift at the frequency domain

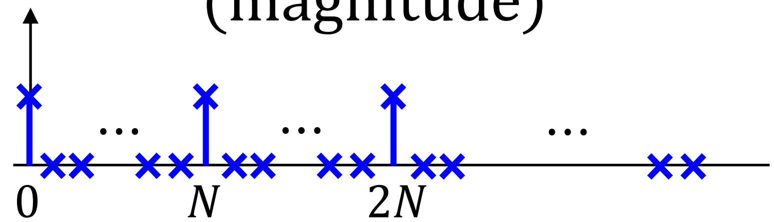


Proof - continued

Time domain

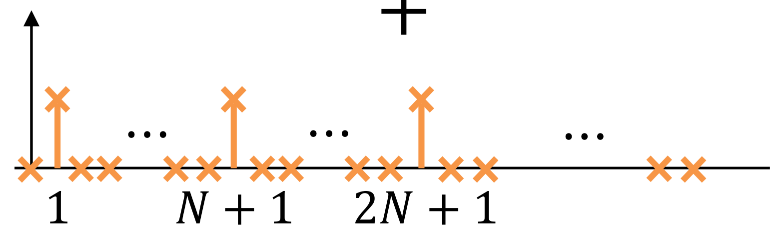
Frequency domain (magnitude)

$(\boldsymbol{s}_0, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})$ ⟺



$+$ $\qquad$ $+$

$(\mathbf{0}, \boldsymbol{s}_1, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})$ ⟺

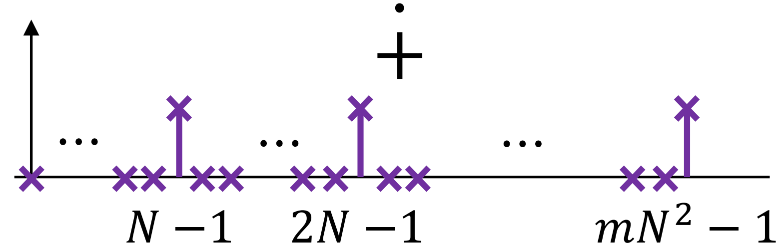


$+$ $\qquad$ $+$

$\vdots$ $\qquad$ $\vdots$

$+$ $\qquad$ $+$

$(\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \boldsymbol{s}_{N-1})$ ⟺



$\|$ $\qquad$ $\|$

$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1})$ ⟺ ?

Proof - done

Time domain

$(\boldsymbol{s}_0, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})$

$+$

$(\mathbf{0}, \boldsymbol{s}_1, \mathbf{0}, \mathbf{0}, \dots, \mathbf{0})$

$+$

$\vdots$

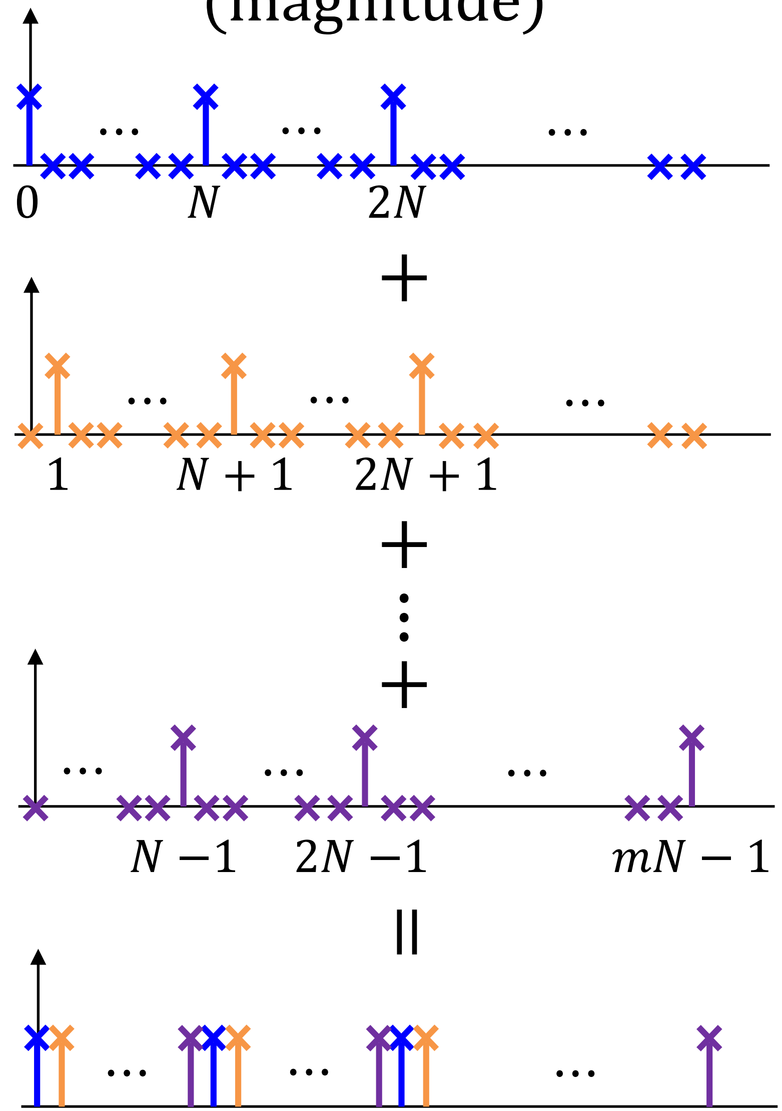
$+$

$(\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}, \boldsymbol{s}_{N-1})$

$||$

$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \dots, \boldsymbol{s}_{N-1})$

Frequency domain (magnitude)



Flat

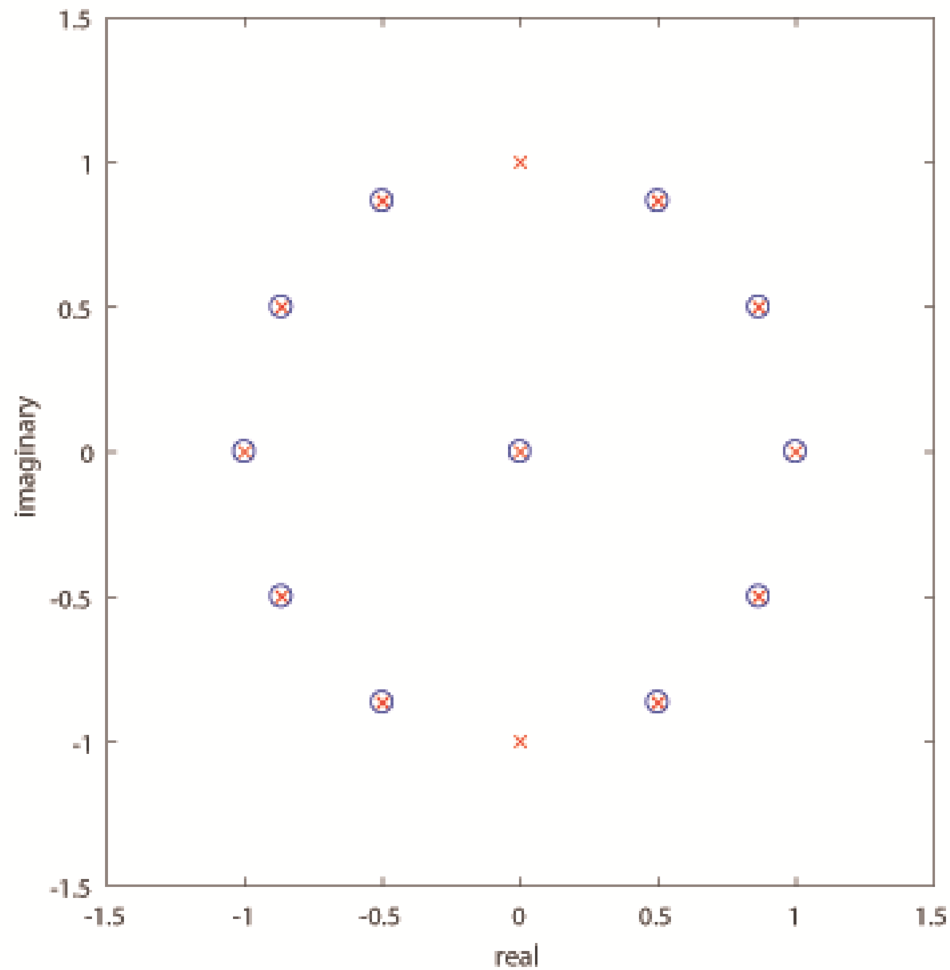
Examples

$\{0, -1, 1, 0, 1, 1\}$ $N = 2$ all-one

Generalized Milewski Construction

$\boldsymbol{s} =$
$\{0, 0, -1, -\omega, 1, \omega^2, 0, 0, 1, \omega^4, 1, \omega^5, 0, 0, -1, -\omega^7, 1, \omega^8, 0, 0, 1, \omega^{10}, 1, \omega^{11}\}$

※ ω is a 12-th primitive root of unity



Constellation of $\boldsymbol{s}$: 12-PSK+

Examples (cont')

$\{3, -2, 3, -2, -2,$
$3, -2, -7, -2, -2\}$
of period 9

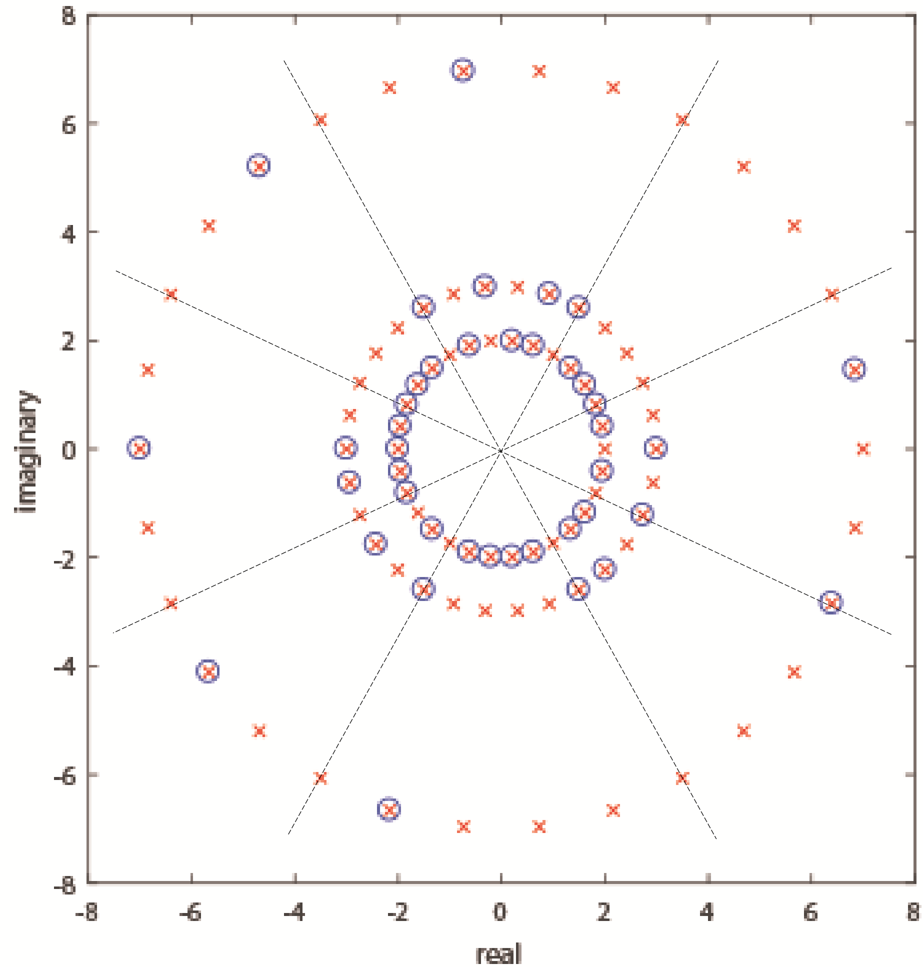
$N = 3$

all-one

Generalized Milewski Construction

$\boldsymbol{s}$ is a perfect sequence of period 90

Phases are aligned



Constellation of $\boldsymbol{s}$: APSK
(3 different amplitudes & 30 different phases)

How many different phases?

※ ω is an mN-th primitive root of unity

$$
\begin{array}{lcl lcl c lcl}
\alpha(0) & \times & (\omega^0)^0 & \alpha(0) & \times & (\omega^1)^0 & \cdots & \alpha(0) & \times & (\omega^{N-1})^0 \\
\alpha(1) & \times & (\omega^0)^1 & \alpha(1) & \times & (\omega^1)^1 & \cdots & \alpha(1) & \times & (\omega^{N-1})^1 \\
\alpha(2) & \times & (\omega^0)^2 & \alpha(2) & \times & (\omega^1)^2 & \cdots & \alpha(2) & \times & (\omega^{N-1})^2 \\
 & \vdots & & & \vdots & & \ddots & & \vdots & \\
\alpha(m-1) & \times & (\omega^0)^{m-1} & \alpha(m-1) & \times & (\omega^1)^{m-1} & \cdots & \alpha(m-1) & \times & (\omega^{N-1})^{m-1} \\
 & \vdots & & & \vdots & & \ddots & & \vdots & \\
\alpha(0) & \times & (\omega^0)^{m(N-1)} & \alpha(0) & \times & (\omega^1)^{m(N-1)} & \cdots & \alpha(0) & \times & (\omega^{N-1})^{m(N-1)} \\
\alpha(1) & \times & (\omega^0)^{m(N-1)+1} & \alpha(1) & \times & (\omega^1)^{m(N-1)+1} & \cdots & \alpha(1) & \times & (\omega^{N-1})^{m(N-1)+1} \\
\alpha(2) & \times & (\omega^0)^{m(N-1)+2} & \alpha(2) & \times & (\omega^1)^{m(N-1)+2} & \cdots & \alpha(2) & \times & (\omega^{N-1})^{m(N-1)+2} \\
 & \vdots & & & \vdots & & \ddots & & \vdots & \\
\alpha(m-1) & \times & (\omega^0)^{mN-1} & \alpha(m-1) & \times & (\omega^1)^{mN-1} & \cdots & \alpha(m-1) & \times & (\omega^{N-1})^{mN-1}
\end{array}
$$

***mN* different phases required, in general**

For arbitrary chosen μ

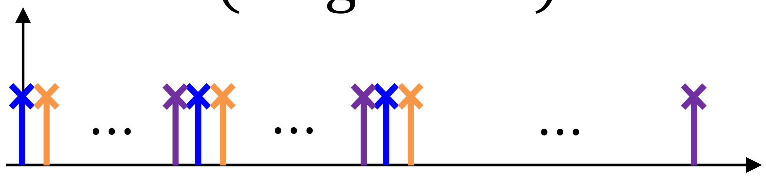
Multiplying a constant $\mu(r)$ with $|\mu(r)| = 1$ to r-th column does not affect the magnitudes of the DFT of

$$(\mathbf{0}, \mathbf{0}, \dots, \mu(r)\boldsymbol{s}_r, \mathbf{0}, \dots, \mathbf{0}) = \mu(r)(\mathbf{0}, \mathbf{0}, \dots, \boldsymbol{s}_r, \mathbf{0}, \dots, \mathbf{0})$$

Time domain

$(\mu(0)\boldsymbol{s}_0, \mu(1)\boldsymbol{s}_1, \dots, \mu(N-1)\boldsymbol{s}_{N-1})$

Frequency domain (magnitude)

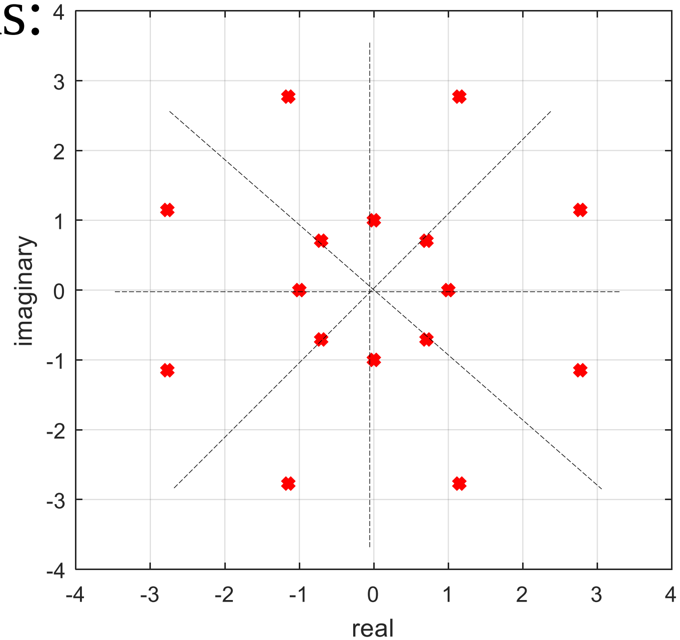


still flat !

Concluding remarks

- The Milewski construction is generalized in period and constellation
  - flexible period, various input sequences
  - perfect sequences over PSK, PSK+, APSK+
    - Example: Input perfect over ASK+ ➔ Output perfect over APSK+

- Some interesting questions for future works:
  - **Possible to reduce the number of phase?**
    - mN different phases, in general.
    - related to QAM constellation
  - **For APSK, how to tilt points?**
    - Two points on circles of different radius have different phase offset to maximize distance, in practice.



After this presentation is accepted,
we have realized that
the construction in this paper can
be further generalized.

I will use just 2 more slides
to show this result briefly,
if it is allowed

Further generalization

recent result

multiset of N perfect sequence of period m (with the same energy)

$\{\boldsymbol{\alpha}_0, \boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_{N-1}\}$

A positive integer

N

A polyphase sequence of length N

$\boldsymbol{\mu}$

A map $f : \mathbb{Z}_N \to \mathbb{Z}_{mN}$ which satisfies $f(x) \neq f(y) (mod\ N)$ for $x \neq y$

f

Further Generalized Milewski Construction

Output **perfect** sequence

$$\boldsymbol{s} = \{s(n)\}_{n=0}^{mN^2-1}$$

where

$$s(n) = \mu(r)\alpha_r(q)\omega^{qf(r)}$$

with $n = qN + r$, and ω is an mN-th primitive root of unity

Relationship with Mow's conjecture

Perfect polyphase sequences

= Further Generalized Milewski construction for only polyphase sequences

Further Generalized Milewski construction with Zadoff-Chu sequences of square-free period

(= Mow's unified construction)

Generalized Milewski construction in this presentation (polyphase only)

Is the area outside the blue box empty or not?

(open for more than 20 years)

Mow confirmed by computer search that they are empty for period $L \leq 20$, # of phase $M \leq 15$, and $L^M \leq 11^{11}$