Rudin-Shapiro-Like Sequences with Low Correlation

Daniel J. Katz, Sangman Lee, and Stanislav A. Trunov
Department of Mathematics
California State University, Northridge

Supported by National Science Foundation Grant DMS 1247679
Computing Resources provided by the Open Science Grid
(supported by NSF award 1148698 and DOE Office of Science)

Open Science Grid All Hands Meeting
University of Utah, Salt Lake City
20 March 2018

Binary Sequences

Binary Sequence: sequence of elements from $\{-1, +1\}$:

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^{\ell}$$

Our sequences are finite length: the above has length ℓ

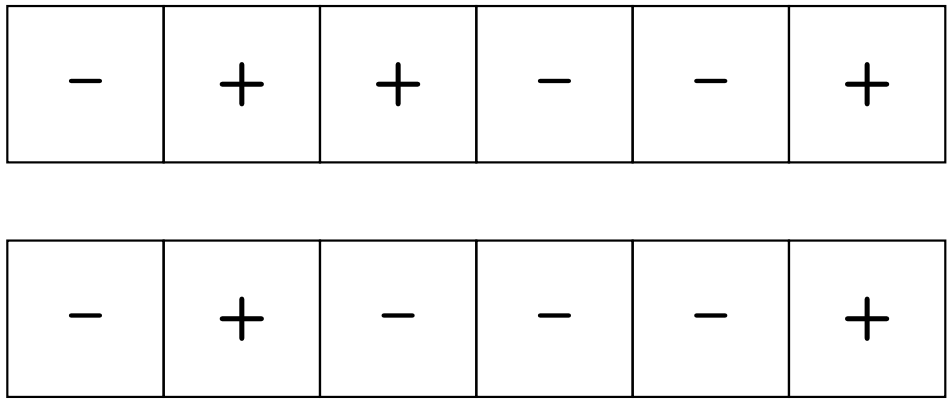
A binary sequence of length 6:

$$\mathbf{(-1,\ +1,\ +1,\ -1,\ -1,\ +1)}$$

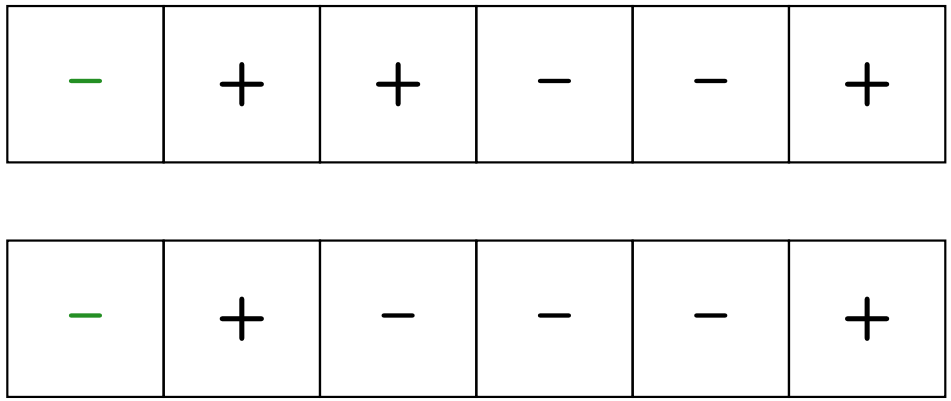
We do not write the 1's, just the signs:

−	+	+	−	−	+

Correlation: Inner Product Measuring Similarity



Correlation: Inner Product Measuring Similarity



$+1$

Correlation: Inner Product Measuring Similarity

−	+	+	−	−	+

−	+	−	−	−	+

$+1 \quad +1$

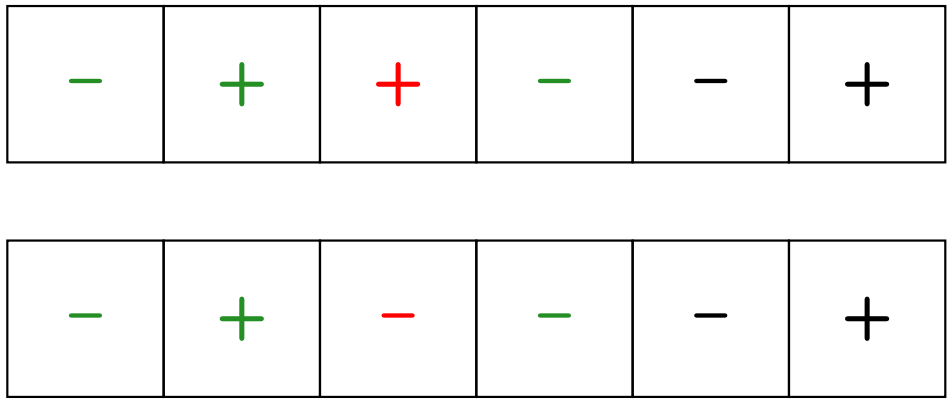
Correlation: Inner Product Measuring Similarity

−	+	+	−	−	+

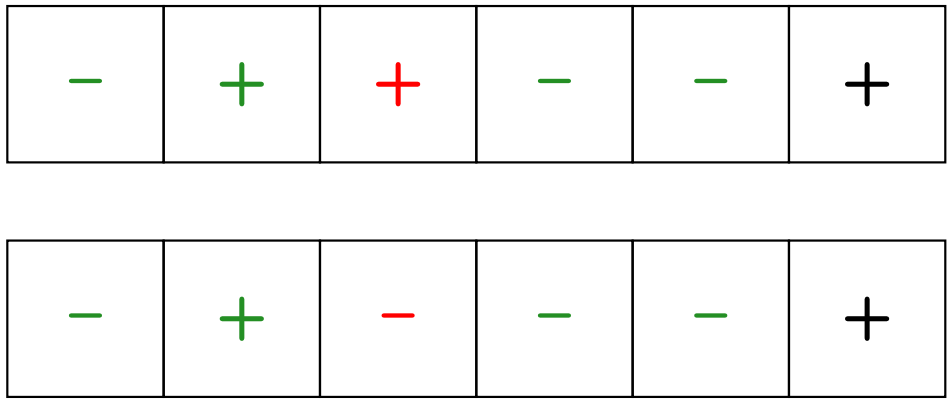
−	+	−	−	−	+

$+1 \quad +1 \quad -1$

Correlation: Inner Product Measuring Similarity



Correlation: Inner Product Measuring Similarity



Correlation: Inner Product Measuring Similarity

−	+	+	−	−	+

−	+	−	−	−	+

+1 +1 −1 +1 +1 +1

Correlation: Inner Product Measuring Similarity

−	+	+	−	−	+

−	+	−	−	−	+

$$+1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad = \quad +4$$

5 Agreements: score $+5$

1 Disagreement: score -1

Overall Score: $(+5) + (-1) = +4$

Correlation: Inner Product Measuring Similarity

−	+	+	−	−	+

−	+	−	−	−	+

$$+1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad = \quad +4$$

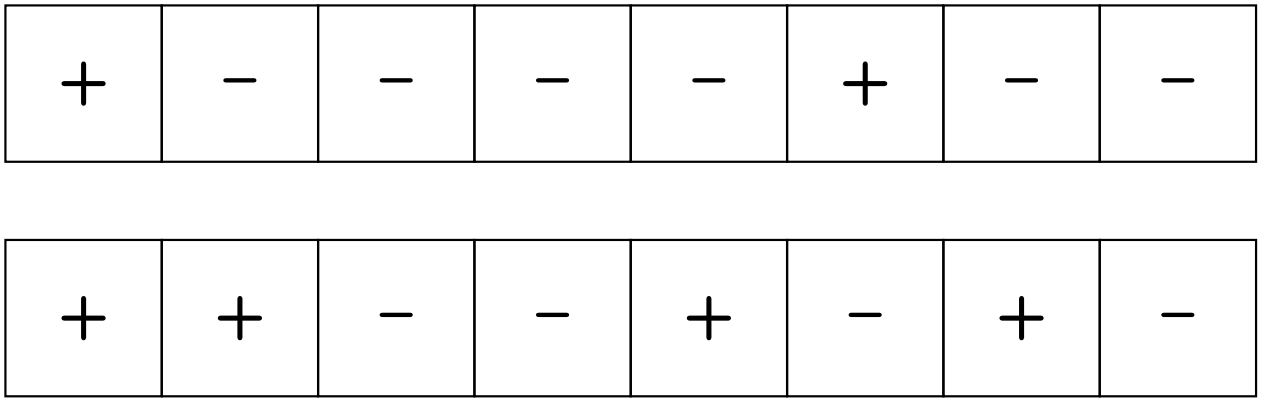
5 Agreements: score $+5$

1 Disagreement: score -1

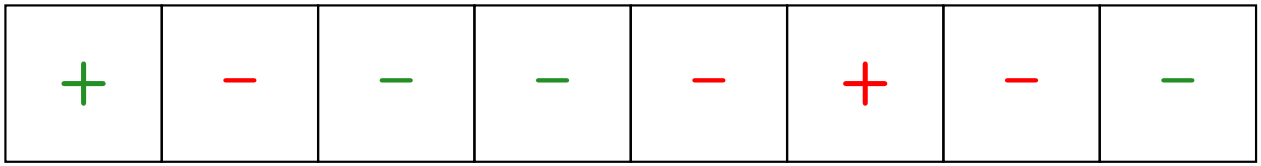
Overall Score: $(+5) + (-1) = +4$

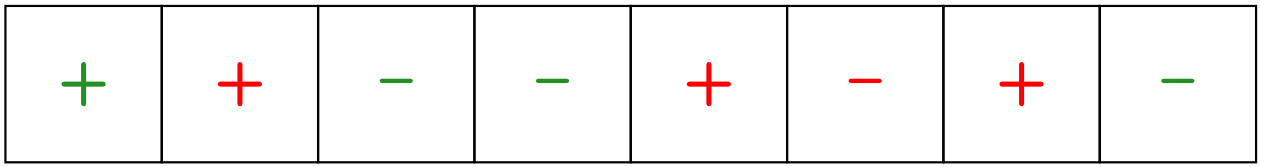
Overall Score $+4$ indicates significant agreement

Shifting



Shifting





Shifting

+	−	−	−	−	+	−	−

+	+	−	−	+	−	+	−

$$+1 \quad -1 \quad +1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad = \quad 0$$

Unshifted Correlation: 0 (no resemblance)

Shifting

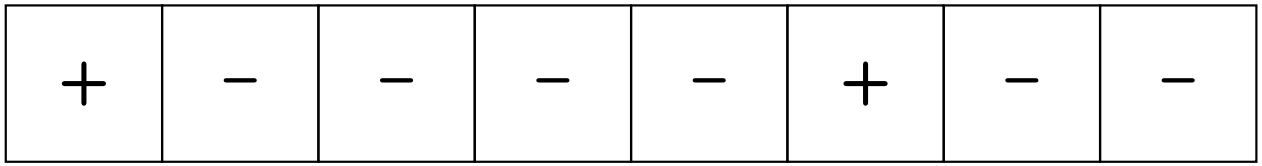
+	−	−	−	−	+	−	−

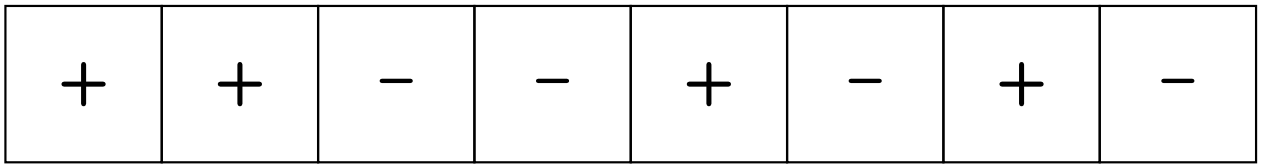
+	+	−	−	+	−	+	−

Unshifted Correlation: 0 (no resemblance)

Shifting

Top sequence is shifted one place to the right



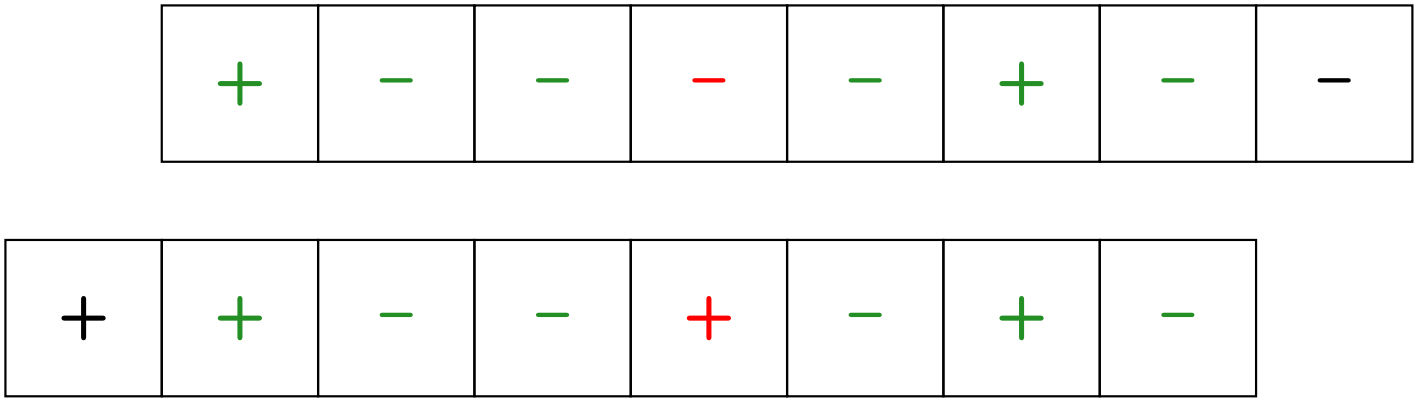


Unshifted Correlation: 0 (no resemblance)

Aperiodic Shifting: ignore non-overlapping portions

Shifting

Top sequence is shifted one place to the right



$$+1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \qquad = \quad +5$$

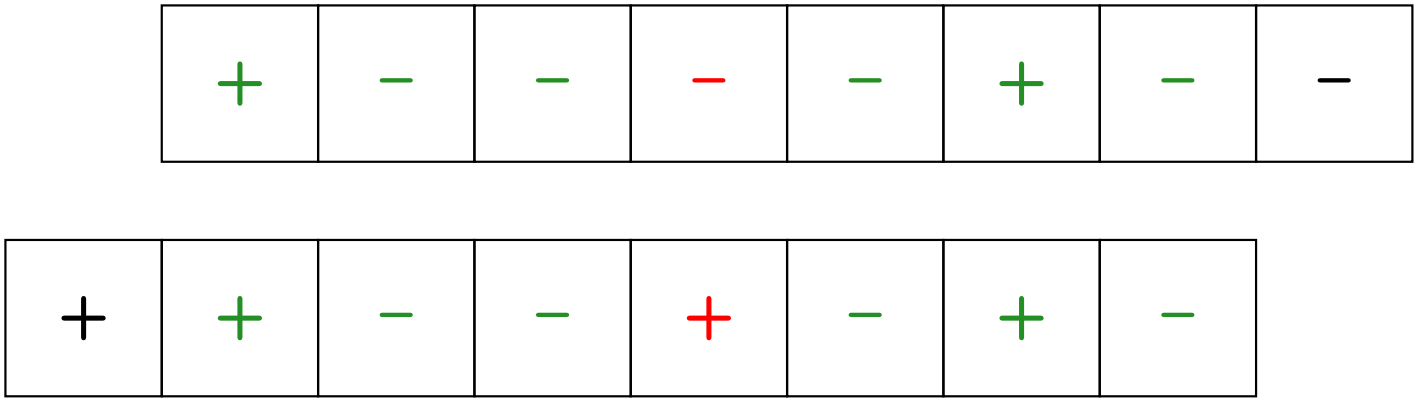
Unshifted Correlation: 0 (no resemblance)

Aperiodic Shifting: ignore non-overlapping portions

Shifted Correlation: +5 (high resemblance)

Shifting

Top sequence is shifted one place to the right



$$+1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \qquad = \quad +5$$

Unshifted Correlation: 0 (no resemblance)

Aperiodic Shifting: ignore non-overlapping portions

Shifted Correlation: +5 (high resemblance)

Sequences resemble each other when shifted by a shift of +1

Aperiodic Crosscorrelation of Sequences

For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)

Aperiodic Crosscorrelation of Sequences

For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)

Aperiodic Crosscorrelation of Sequences

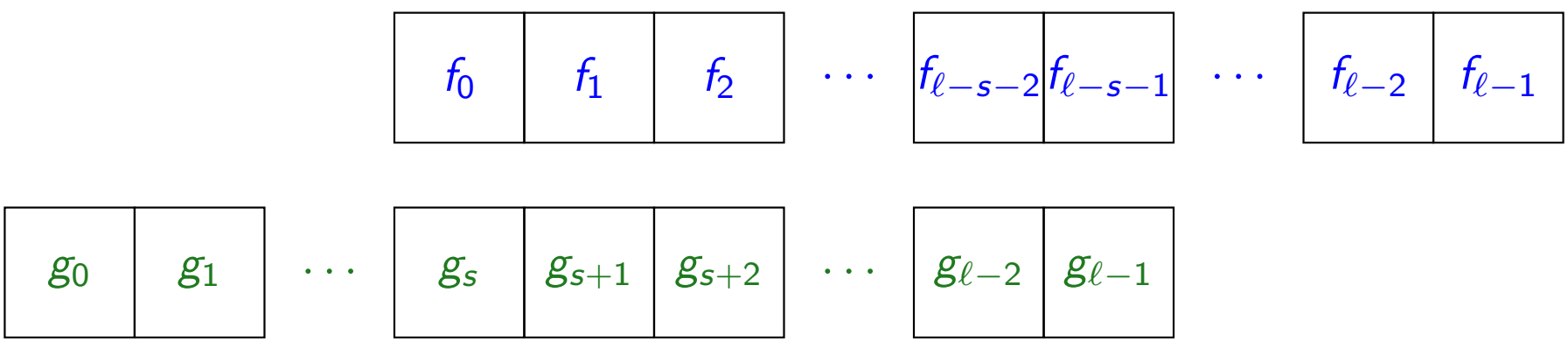
For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)



Aperiodic Crosscorrelation of Sequences

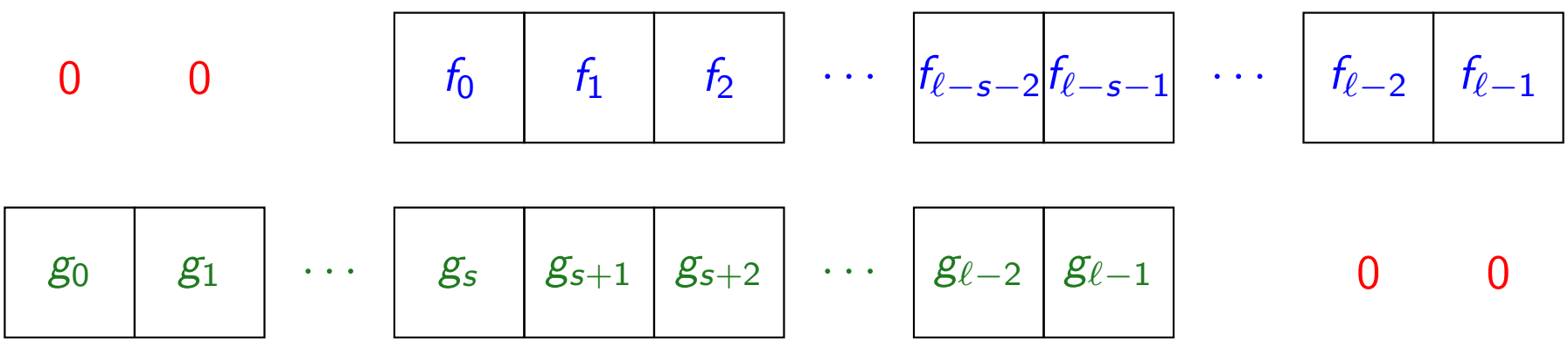
For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)



Aperiodic Crosscorrelation of Sequences

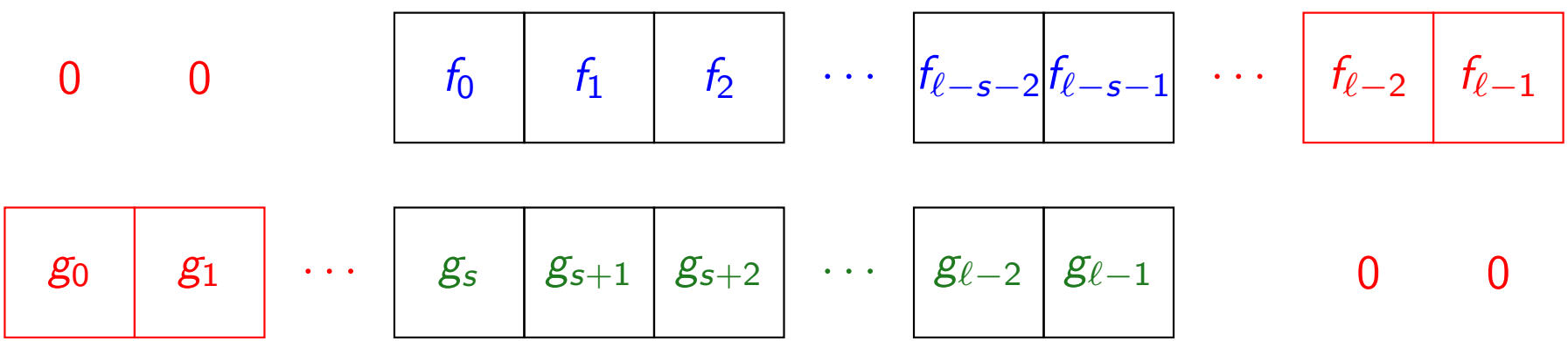
For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)



Aperiodic Crosscorrelation of Sequences

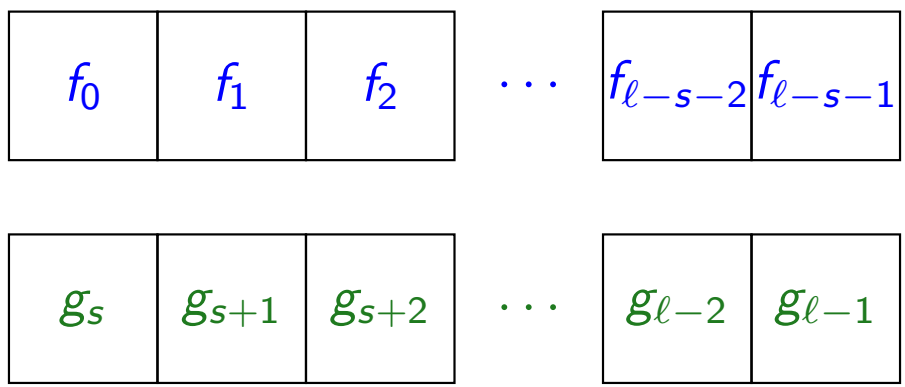
For two sequences

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{-1, +1\}^\ell$$
$$g = (g_0, g_1, \ldots, g_{\ell-1}) \in \{-1, +1\}^\ell$$

Aperiodic crosscorrelation of f with g at shift s (for any integer s):

$$C_{f,g}(s) = \sum_{j=-\infty}^{\infty} f_j \, g_{j+s}$$

(where we consider $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)



Autocorrelation

Aperiodic Autocorrelation = aperiodic crosscorrelation of a sequence with itself; for

$$f = (f_0, f_1, \ldots, f_{\ell-1}) \in \{+1, -1\}^\ell$$

the autocorrelation of f at shift s is

$$C_{f,f}(s) = \sum_{j=-\infty}^{\infty} f_j \, f_{j+s}$$

(where we consider $f_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$)

Since our $f_0, \ldots, f_{\ell-1}$ are $+1$'s and -1's, at shift $s = 0$

$$C_{f,f}(0) = \sum_{j=-\infty}^{\infty} {f_j}^2 = \sum_{j=0}^{\ell-1} {f_j}^2 = \ell = \text{ length of sequence } f$$

Design Goal

Our sensors can only measure the absolute value of the correlation

Goal: We want pairs of binary sequences (f, g) with

- Low autocorrelation for f:
  $|C_{f,f}(s)|$ small for all $s \neq 0$
  (recall $|C_{f,f}(0)|$ = length of f = large)

  Assists synchronization for f
- Low autocorrelation for g:
  $|C_{g,g}(s)|$ small for all $s \neq 0$
  (recall $|C_{g,g}(0)|$ = length of g = large)

  Assists synchronization for g
- Low crosscorrelation between f and g:
  $|C_{f,g}(s)|$ small for all s

  Prevents confusion of f with g

Demerit and Merit Factors

Use sum of squared magnitudes compared to sequence length ℓ to measure overall smallness of correlation

Crosscorrelation demerit factor of sequences f and g:

$$\mathrm{CDF}(f,g) = \frac{\sum_{s=-\infty}^{\infty} |C_{f,g}(s)|^2}{\ell^2}$$

Crosscorrelation merit factor

$$\mathrm{CMF}(f,g) = \frac{1}{\mathrm{CDF}(f,g)}$$

Autocorrelation demerit factor of sequence f:

$$\mathrm{ADF}(f) = \frac{\sum_{\substack{s=-\infty \\ s\neq 0}}^{\infty} |C_{f,f}(s)|^2}{\ell^2} = \mathrm{CDF}(f,f) - 1$$

Autocorrelation merit factor

$$\mathrm{AMF}(f) = \frac{1}{\mathrm{ADF}(f)}$$

Typical Demerit Factors

Sarwate (1984) calculated expected values of demerit factors

for randomly selected binary sequences f of length ℓ:

Average autocorrelation demerit factor

$$E[\mathrm{ADF}(f)] = 1 - \frac{1}{\ell}$$

Average crosscorrelation demerit factor for sequences f and g of length ℓ:

$$E[\mathrm{CDF}(f, g)] = 1$$

So typical values will be 1 for both autocorrelation and crosscorrelation when ℓ is large.

Pursley-Sarwate Criterion

For binary sequences f and g, Pursley and Sarwate (1976) proved

$$\sqrt{\mathrm{ADF}(f)\,\mathrm{ADF}(g)} + \mathrm{CDF}(f,g) \geq 1$$

The proof is based on the Cauchy-Schwarz inequality

We define the *Pursley-Sarwate Criterion*

$$\mathrm{PSC}(f,g) = \sqrt{\mathrm{ADF}(f)\,\mathrm{ADF}(g)} + \mathrm{CDF}(f,g)$$

For typical randomly selected sequence pairs, we expect

$$\mathrm{PSC}(f,g) \approx 2$$

Goal: make $\mathrm{PSC}(f,g)$ as close to 1 as possible

Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

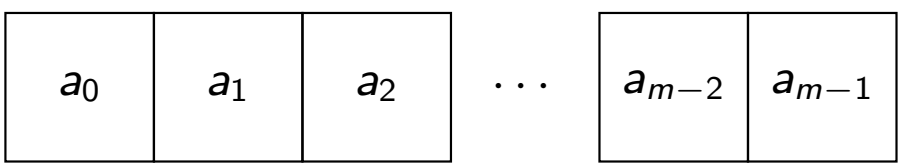
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

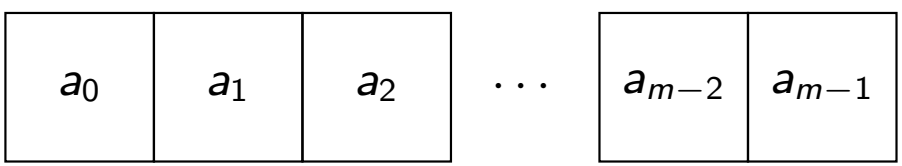
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

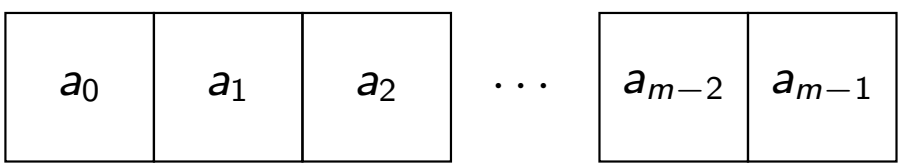
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

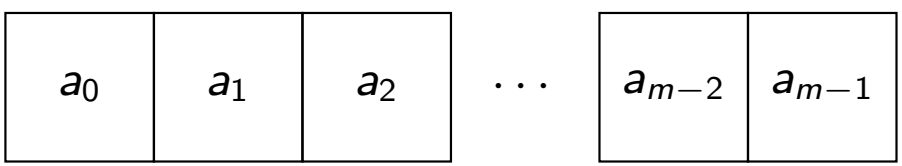
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

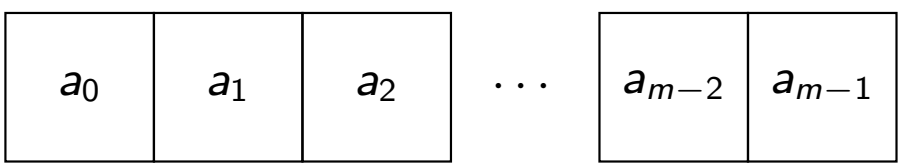
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

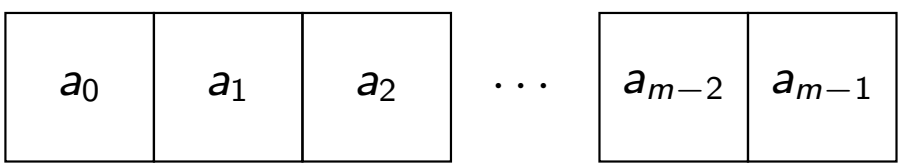
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined,



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

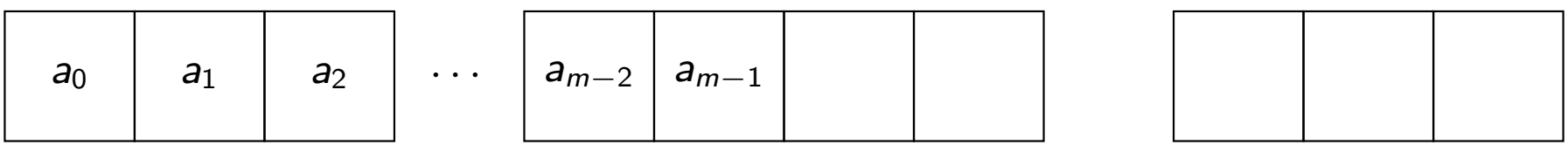
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

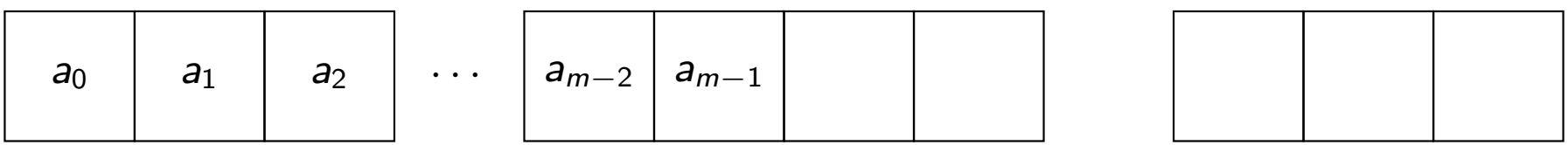
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

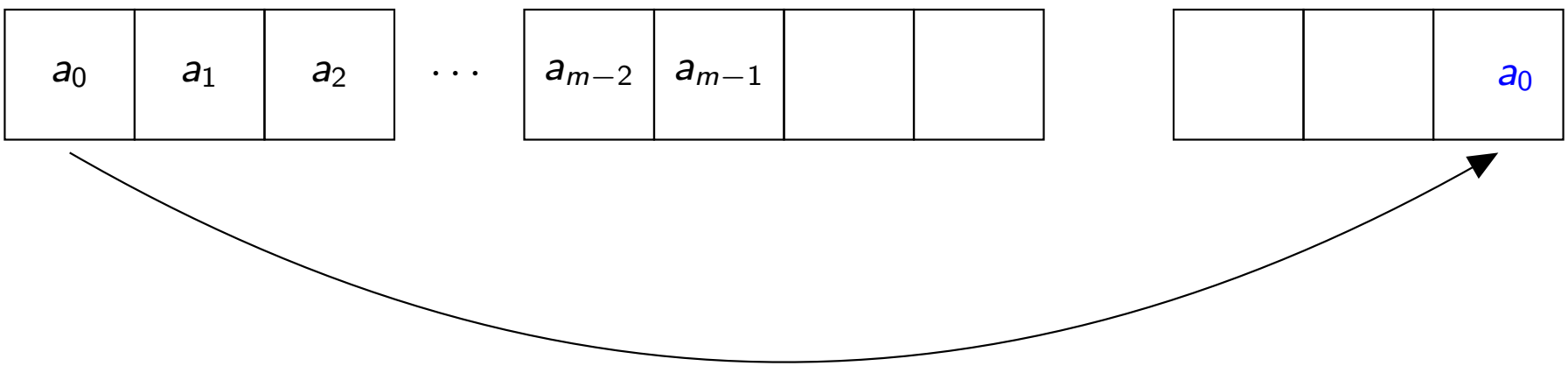
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

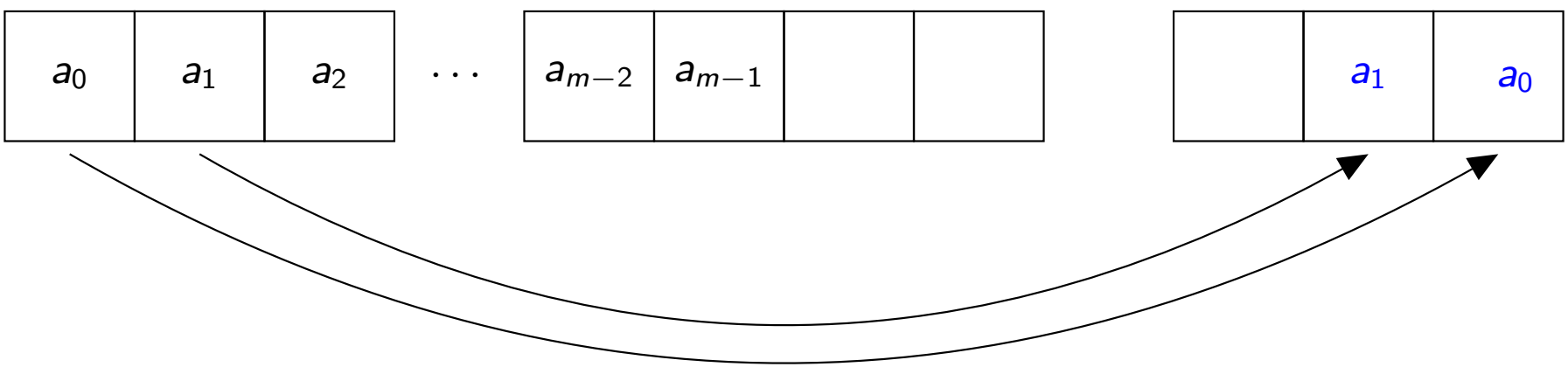
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

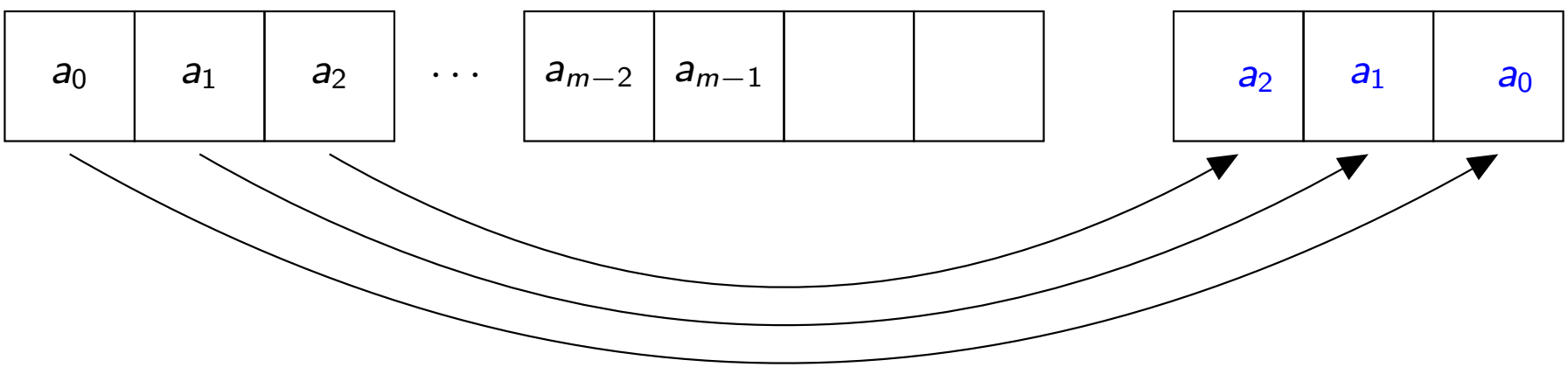
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

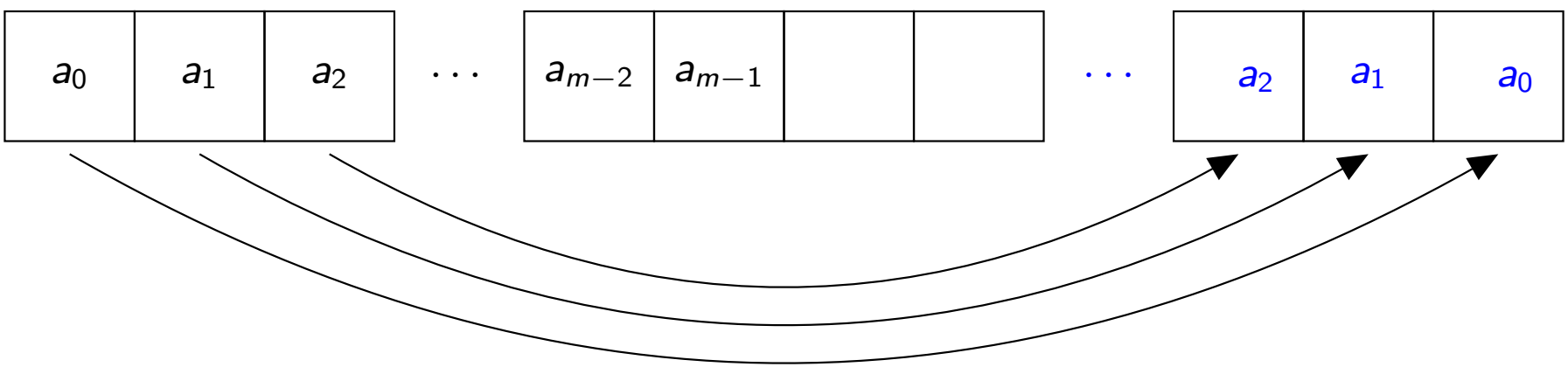
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

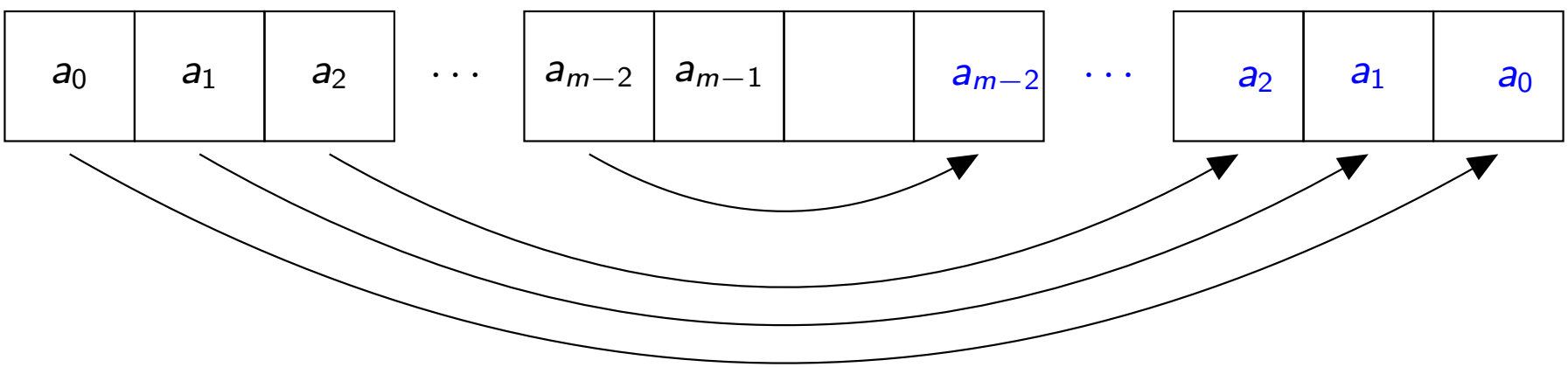
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

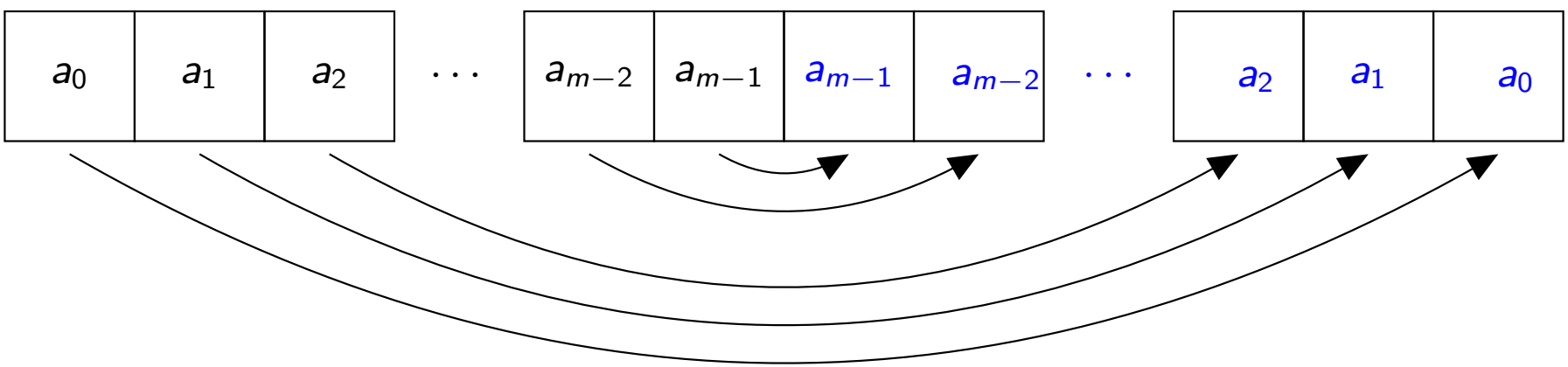
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

reverse the first half



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

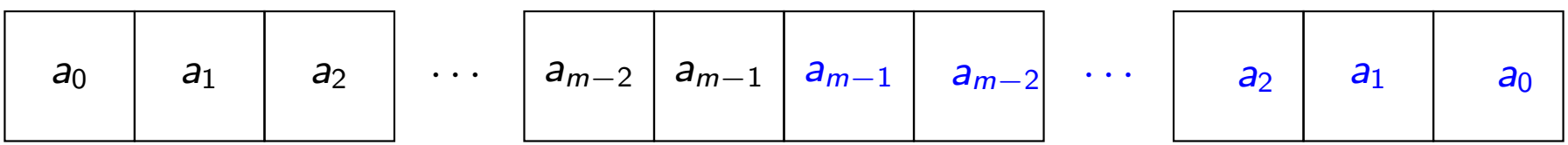
$$f^0, f^1, f^2, \ldots$$

where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

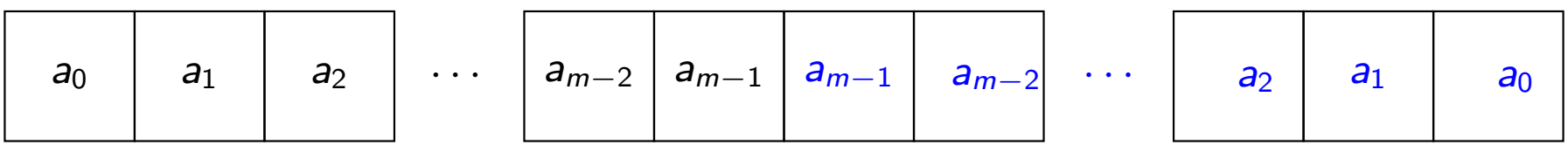
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

change half the signs



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

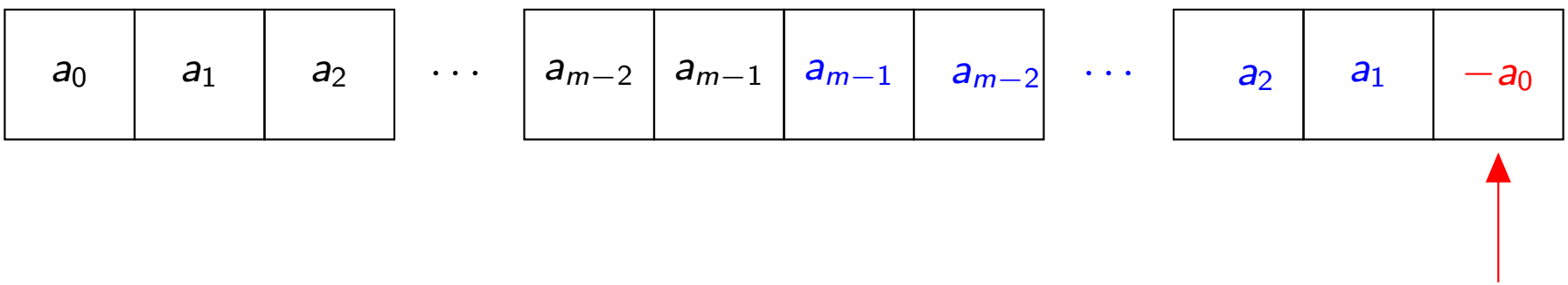
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

change half the signs



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

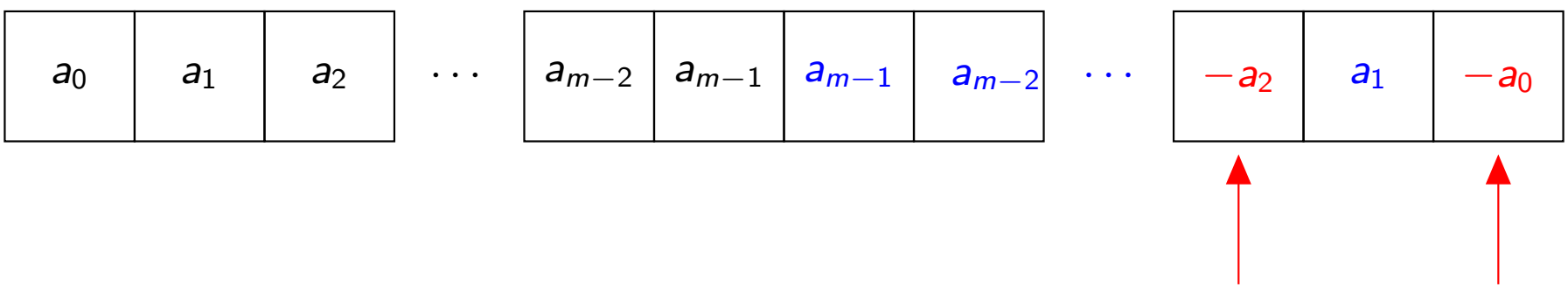
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

change half the signs



Rudin-Shapiro-Like Sequences

Rudin-Shapiro-Like Sequences come in families of the form

$$f^0, f^1, f^2, \ldots$$

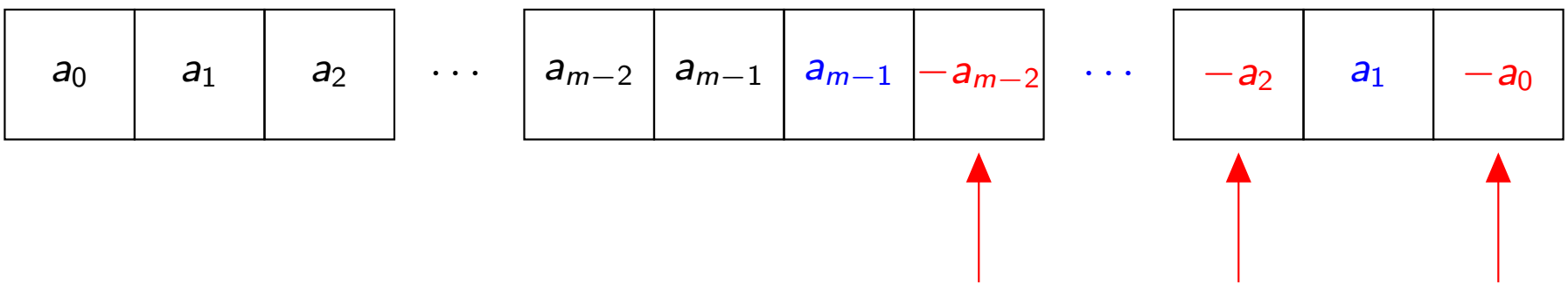
where the length of f^{n+1} is double that of f^n.

- The initial sequence f^0 is called the seed sequence
- The family of sequences $f^0, f^1, f^2, \ldots$ is called the stem

Construction

- Choose a binary sequence f^0 to be the seed
- Once $f^n = (a_0, a_1, \ldots, a_{m-1})$ is defined, get f^{n+1} by doubling:

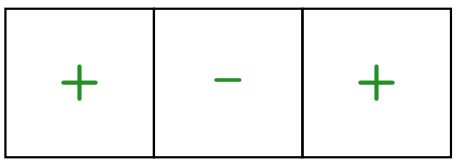
change half the signs



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

f^0



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

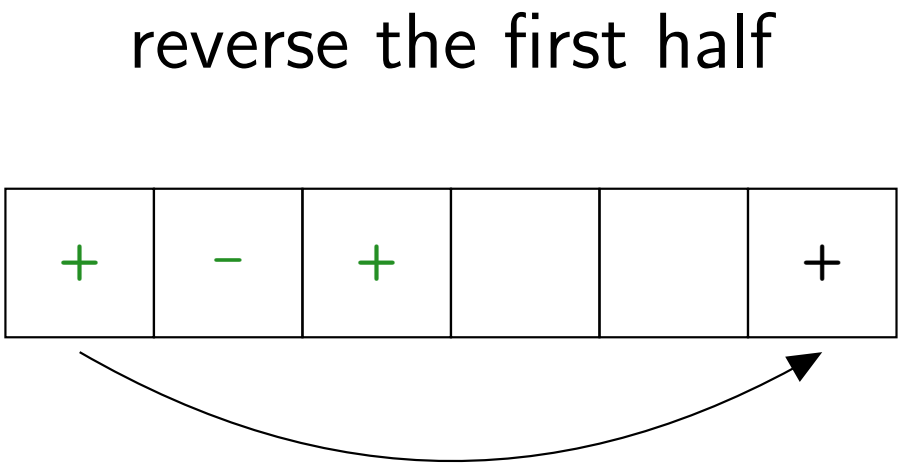
Then we double to get f^1

reverse the first half

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

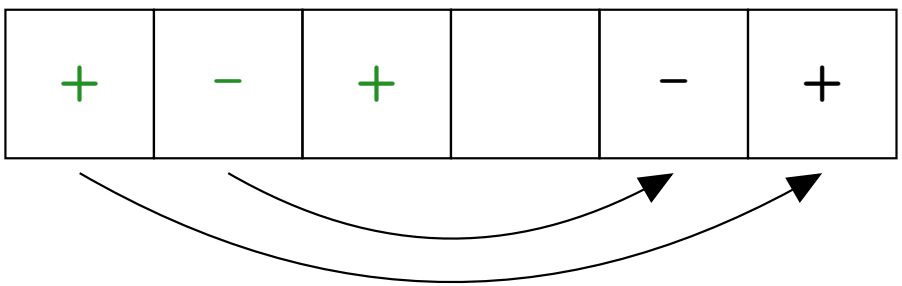


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

reverse the first half

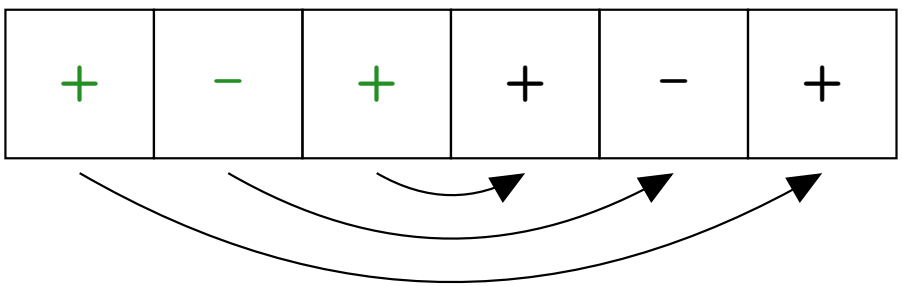


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

reverse the first half



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

change half the signs

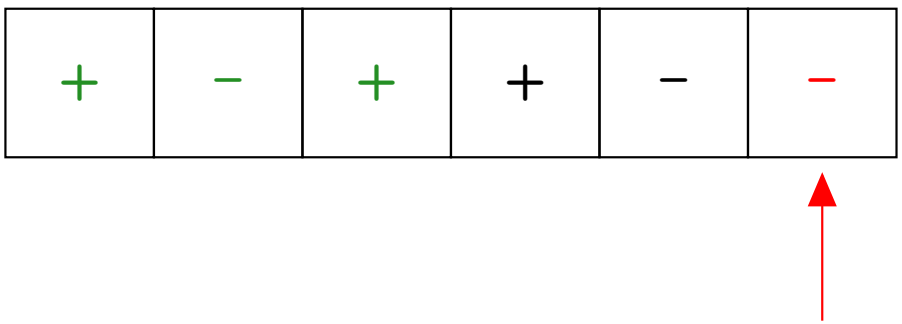
+	−	+	+	−	+

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

change half the signs

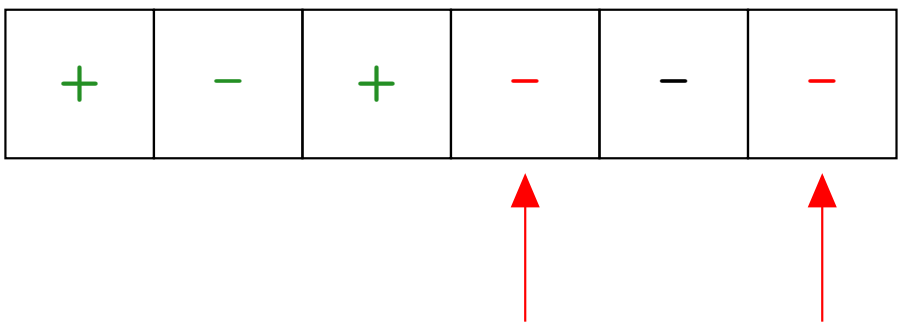


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

change half the signs



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

f^1

+	−	+	−	−	−

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

+	−	+	−	−	−						

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

reverse the first half

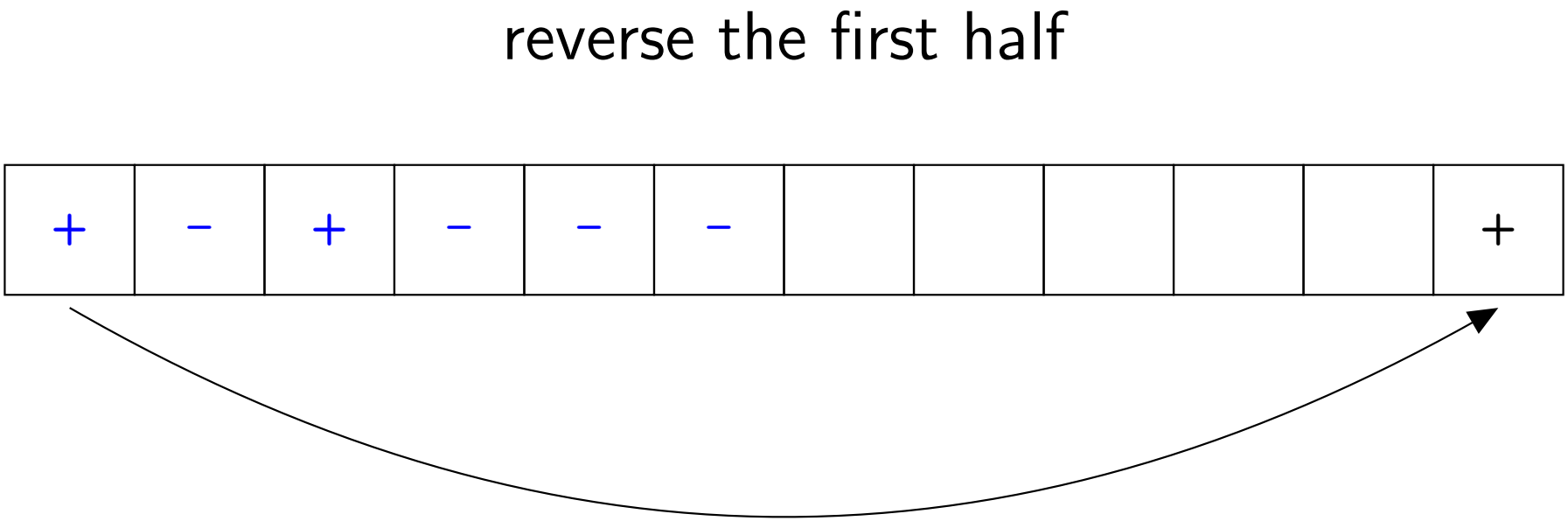
+	−	+	−	−	−						

Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

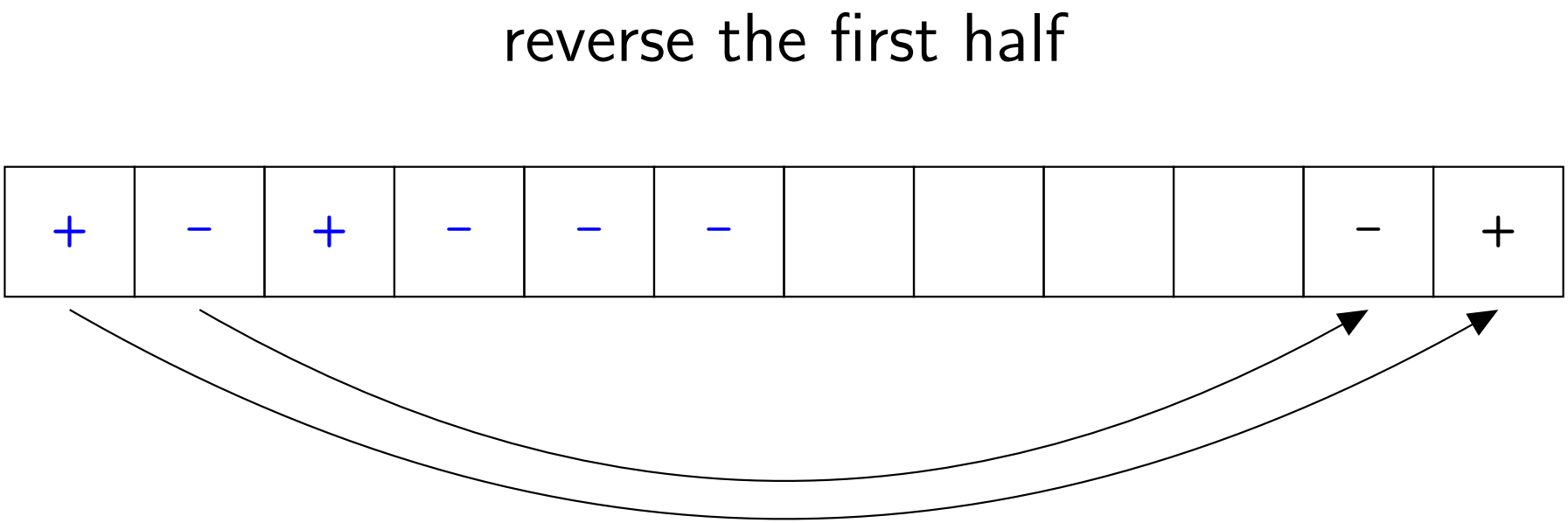


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

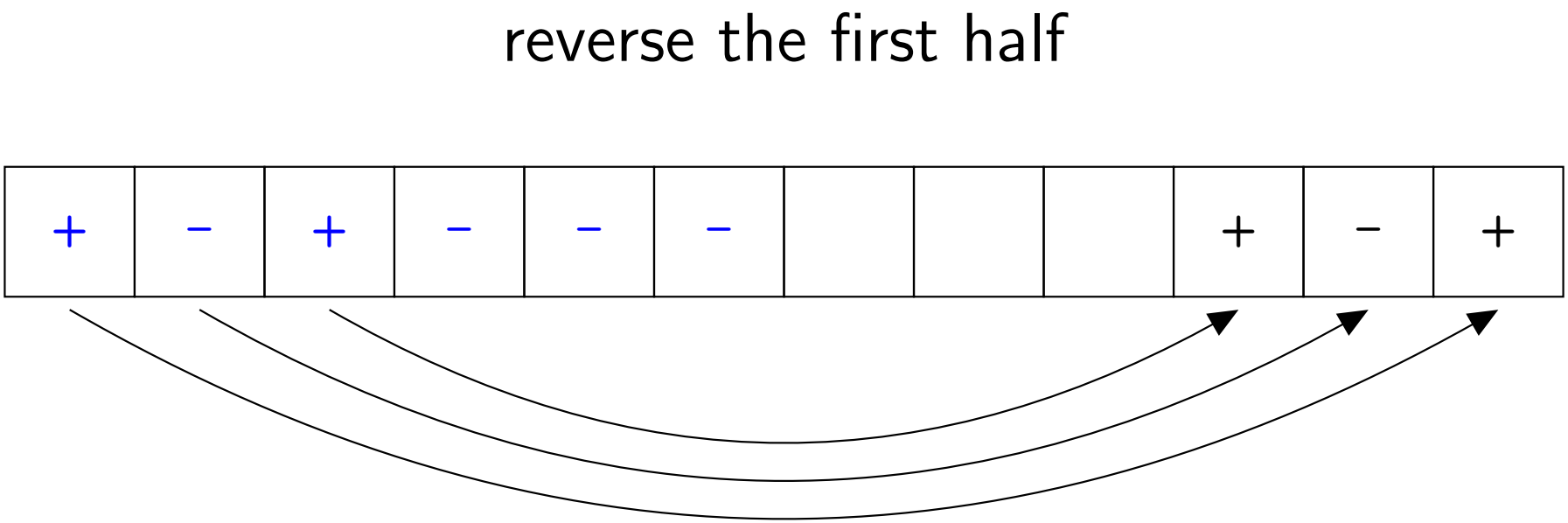


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

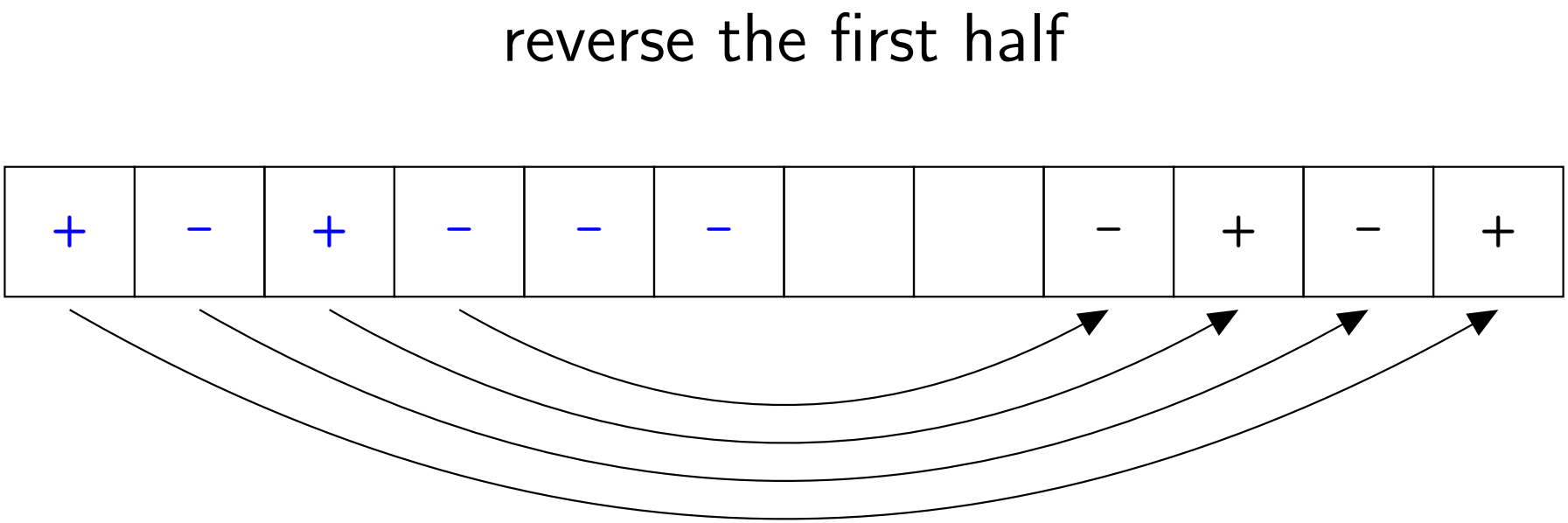


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

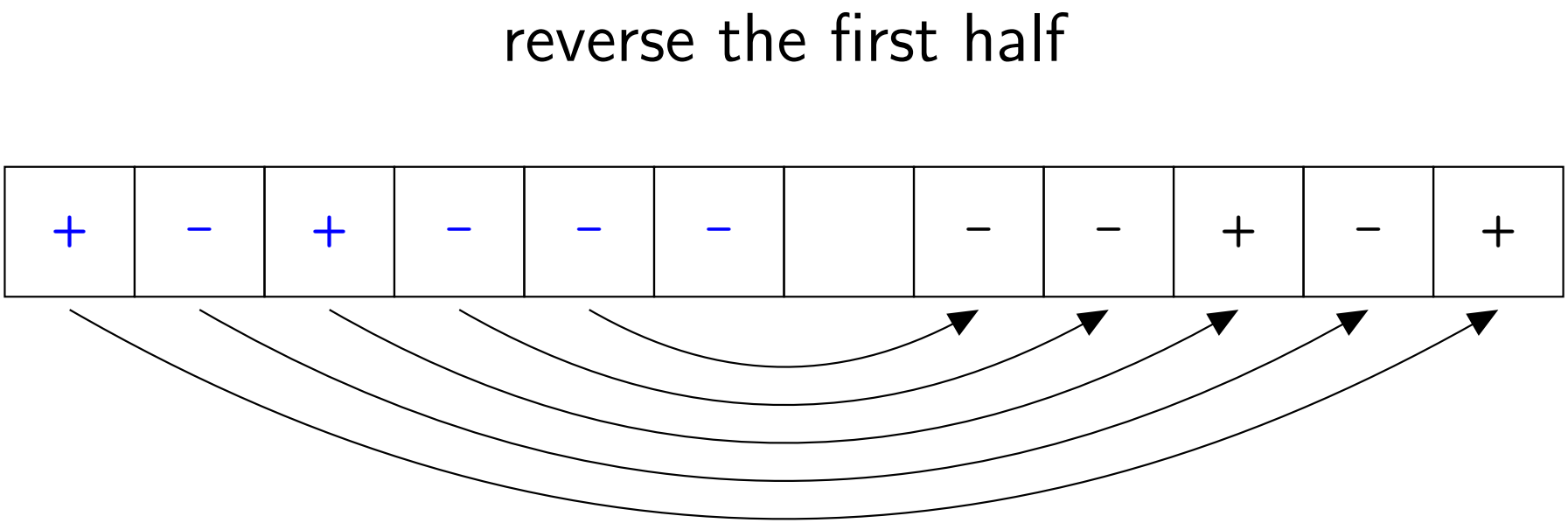


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

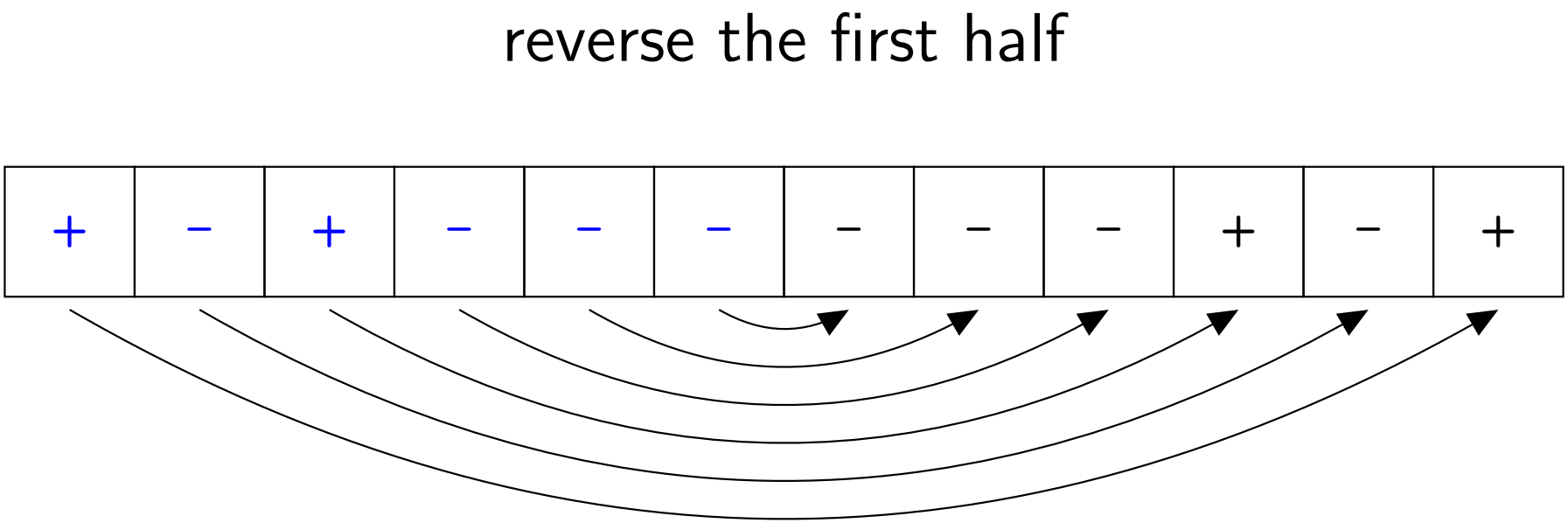


Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

change half the signs

+	−	+	−	−	−	−	−	−	+	−	+

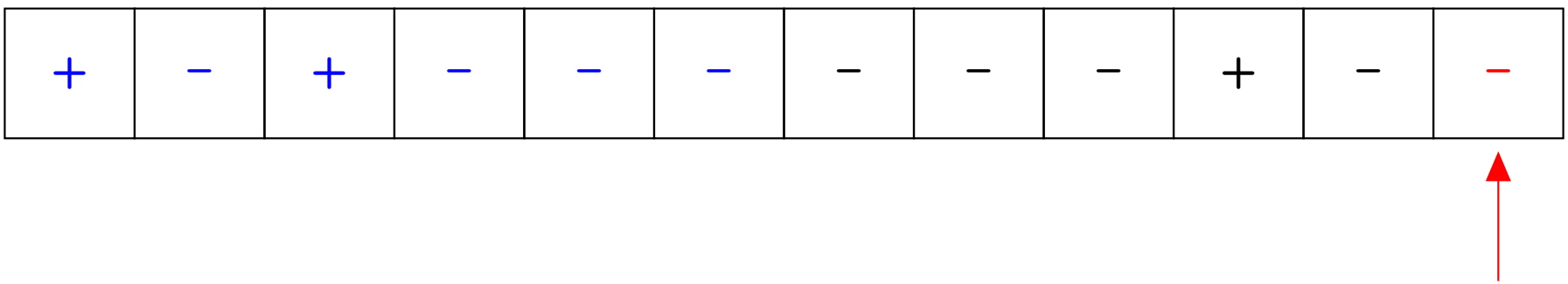
Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

change half the signs



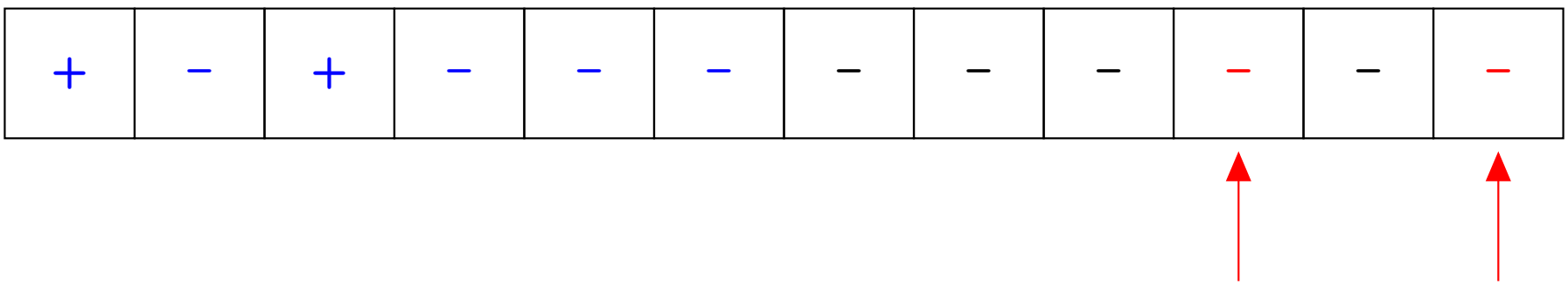
Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

change half the signs



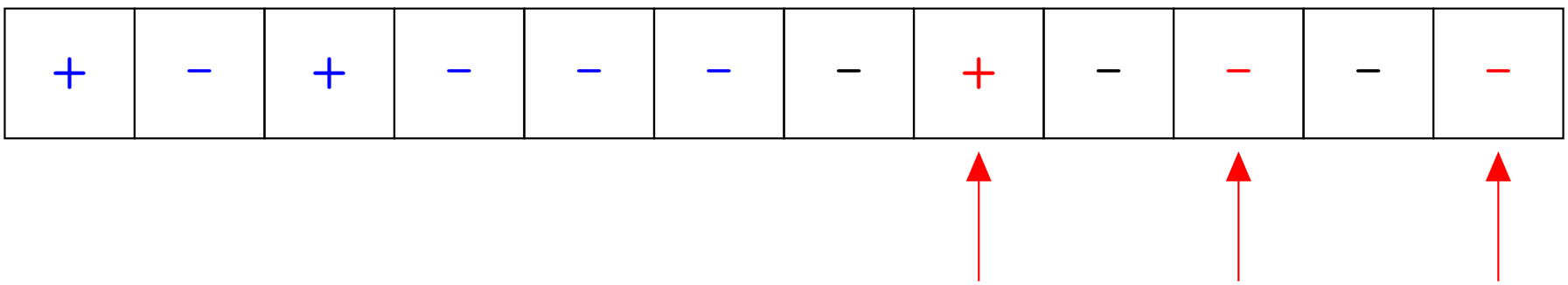
Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

change half the signs



Example of Doubling Construction

Suppose we have the following seed sequence: $f^0 = (+1, -1, +1)$

Then we double to get f^1

Then we double again to get f^2

f^2

+	−	+	−	−	−	−	+	−	−	−	−

Our Idea

- Two seed sequences, f^0 and g^0, of equal length
- Grow f^0 into a stem $f^0, f^1, f^2, \ldots$
- Grow g^0 into a stem $g^0, g^1, g^2, \ldots$
- For each n, determine
  - $\mathrm{ADF}(f^n)$ autocorrelation demerit factor of f^n
  - $\mathrm{ADF}(g^n)$ autocorrelation demerit factor of g^n
  - $\mathrm{CDF}(f^n, g^n)$ crosscorrelation demerit factor of f^n and g^n
  - $\mathrm{PSC}(f^n, g^n)$ Pursley-Sarwate criterion for f^n and g^n

$$\mathrm{PSC}(f^n, g^n) = \sqrt{\mathrm{ADF}(f^n)\mathrm{ADF}(g^n)} + \mathrm{CDF}(f^n, g^n)$$

Recall $\mathrm{PSC}(f^n, g^n) \geq 1$ always

We want to make $\mathrm{PSC}(f^n, g^n)$ as close to 1 as possible

Asymptotic Result

If $f^0, f^1, \ldots$ and $g^0, g^1, \ldots$ are stems, then

Asymptotic Result

If $f^0, f^1, \ldots$ and $g^0, g^1, \ldots$ are stems, then

$$\lim_{n\to\infty} \mathrm{ADF}(f^n) = -1 + \frac{2}{3} \cdot \frac{\|f^0\|_4^4 + \|f^0 \widetilde{f}^0\|_2^2}{\|f^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{ADF}(g^n) = -1 + \frac{2}{3} \cdot \frac{\|g^0\|_4^4 + \|g^0 \widetilde{g}^0\|_2^2}{\|g^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n) = \frac{2\|f^0 g^0\|_2^2 + \|f^0 \widetilde{g}^0\|_2^2 + \mathrm{Re} \int f^0 \widetilde{f}^0 \overline{g^0 \widetilde{g}^0}}{3\|f^0\|_2^2 \|g^0\|_2^2},$$

where we identify sequences with polynomials:

$$a = (a_0, \ldots, a_{\ell-1}) \leftrightarrow a(z) = a_0 + a_1 z + \cdots + a_{\ell-1} z^{\ell-1}$$

and $\widetilde{f}^0(z)$ and $\widetilde{g}^0(z)$ are $f^0(-z)$ and $g^0(-z)$, and

$$\|a\|_p = \left(\frac{1}{2\pi} \int_0^{2\pi} |a(e^{i\theta})|^p d\theta \right)^{1/p}$$

$$\int f^0 \widetilde{f}^0 \overline{g^0 \widetilde{g}^0} = \frac{1}{2\pi} \int_0^{2\pi} f^0(e^{i\theta}) \widetilde{f}^0(e^{i\theta}) \overline{g^0(e^{i\theta}) \widetilde{g}^0(e^{i\theta})} d\theta.$$

Asymptotic Result

If $f^0, f^1, \ldots$ and $g^0, g^1, \ldots$ are stems, then

$$\lim_{n\to\infty} \mathrm{ADF}(f^n) = -1 + \frac{2}{3} \cdot \frac{\|f^0\|_4^4 + \|f^0 \widetilde{f}^0\|_2^2}{\|f^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{ADF}(g^n) = -1 + \frac{2}{3} \cdot \frac{\|g^0\|_4^4 + \|g^0 \widetilde{g}^0\|_2^2}{\|g^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n) = \frac{2\|f^0 g^0\|_2^2 + \|f^0 \widetilde{g}^0\|_2^2 + \mathrm{Re} \int f^0 \widetilde{f}^0 \overline{g^0 \widetilde{g}^0}}{3\|f^0\|_2^2 \|g^0\|_2^2}.$$

Borwein and Mossinghoff showed that $\lim_{n\to\infty} \mathrm{ADF}(f^n) \geq 1/3$, with equality certain seeds of length 1, 2, 4, 8, 16, 20, 32, 40.

Asymptotic Result

If $f^0, f^1, \ldots$ and $g^0, g^1, \ldots$ are stems, then

$$\lim_{n\to\infty} \mathrm{ADF}(f^n) = -1 + \frac{2}{3} \cdot \frac{\|f^0\|_4^4 + \|f^0 \widetilde{f}^0\|_2^2}{\|f^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{ADF}(g^n) = -1 + \frac{2}{3} \cdot \frac{\|g^0\|_4^4 + \|g^0 \widetilde{g}^0\|_2^2}{\|g^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n) = \frac{2\|f^0 g^0\|_2^2 + \|f^0 \widetilde{g}^0\|_2^2 + \mathrm{Re} \int f^0 \widetilde{f}^0 \overline{g^0 \widetilde{g}^0}}{3\|f^0\|_2^2 \|g^0\|_2^2}.$$

Borwein and Mossinghoff showed that $\lim_{n\to\infty} \mathrm{ADF}(f^n) \geq 1/3$, with equality certain seeds of length 1, 2, 4, 8, 16, 20, 32, 40.

We showed that $\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n)$ can be made arbitrarily close to 0, but at the cost of very high autocorrelation.

Asymptotic Result

If $f^0, f^1, \ldots$ and $g^0, g^1, \ldots$ are stems, then

$$\lim_{n\to\infty} \mathrm{ADF}(f^n) = -1 + \frac{2}{3} \cdot \frac{\|f^0\|_4^4 + \|f^0 \widetilde{f}^0\|_2^2}{\|f^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{ADF}(g^n) = -1 + \frac{2}{3} \cdot \frac{\|g^0\|_4^4 + \|g^0 \widetilde{g}^0\|_2^2}{\|g^0\|_2^4},$$

$$\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n) = \frac{2\|f^0 g^0\|_2^2 + \|f^0 \widetilde{g}^0\|_2^2 + \mathrm{Re} \int f^0 \widetilde{f}^0 \overline{g^0 \widetilde{g}^0}}{3\|f^0\|_2^2 \|g^0\|_2^2}.$$

Borwein and Mossinghoff showed that $\lim_{n\to\infty} \mathrm{ADF}(f^n) \geq 1/3$, with equality certain seeds of length 1, 2, 4, 8, 16, 20, 32, 40.

We showed that $\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n)$ can be made arbitrarily close to 0, but at the cost of very high autocorrelation.

In our work, we calculate the limiting Pursley-Sarwate Criterion

$$\lim_{n\to\infty} \mathrm{PSC}(f^n, g^n) = \lim_{n\to\infty} \sqrt{\mathrm{ADF}(f^n)\mathrm{ADF}(g^n)} + \mathrm{CDF}(f^n, g^n)$$

Computational Techniques

Gray code: order the sequences so that successive sequences differ in only one position, e.g.

0	+	+	+	4	−	−	+
1	+	+	−	5	−	−	−
2	+	−	−	6	−	+	−
3	+	−	+	7	−	+	+

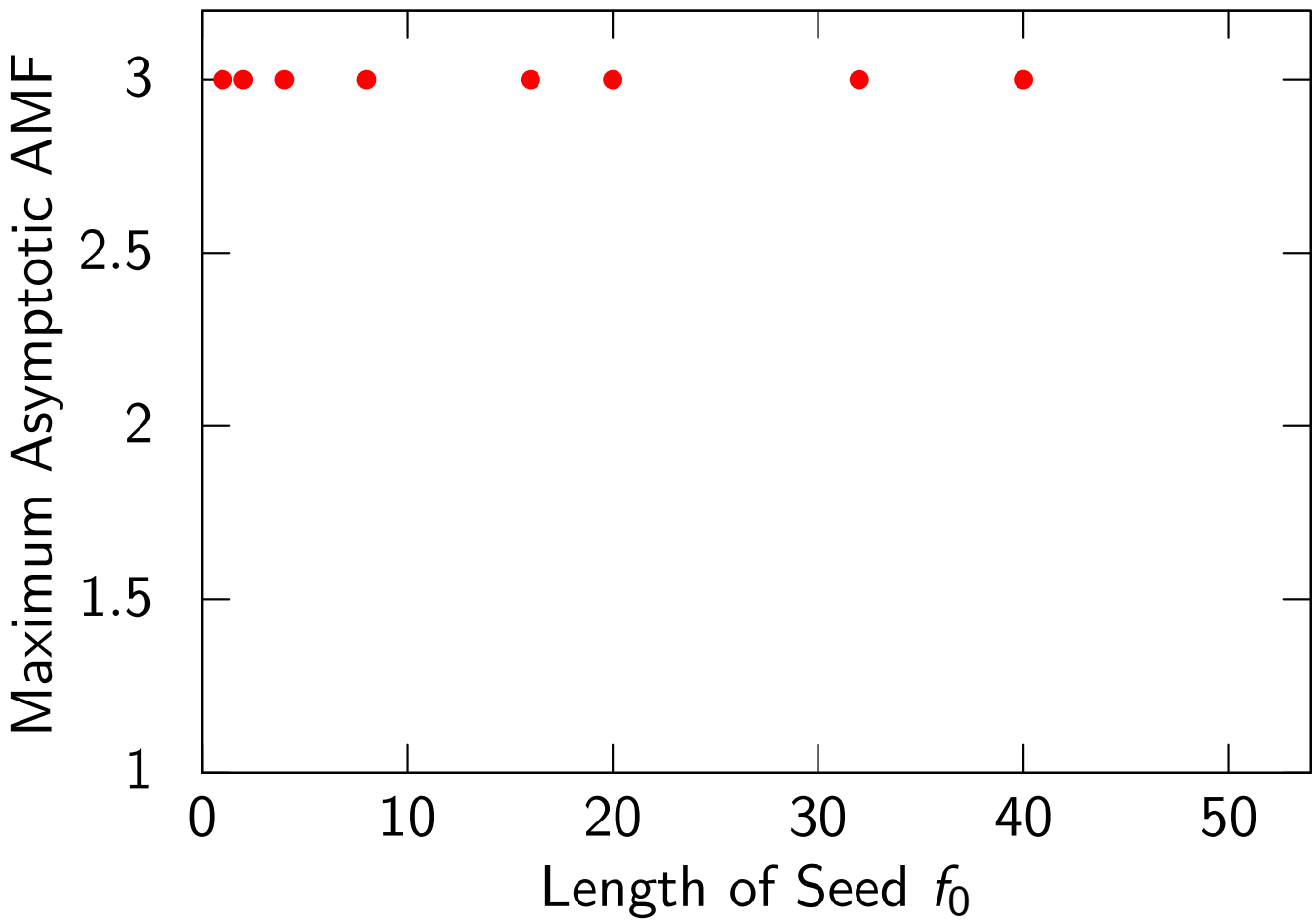
Fourier analysis helps compute the integrals faster

Symmetry helps: exchange sequences, negate either, negate every other term of both, reverse both

- Overall a group G of order 32 of symmetries preserves limiting PSC for seeds of length > 1
- Odd seed lengths: $G \cong D_8 \times C_2 \times C_2$
- Even seed lengths: extraspecial group, order 2^5, type $+$

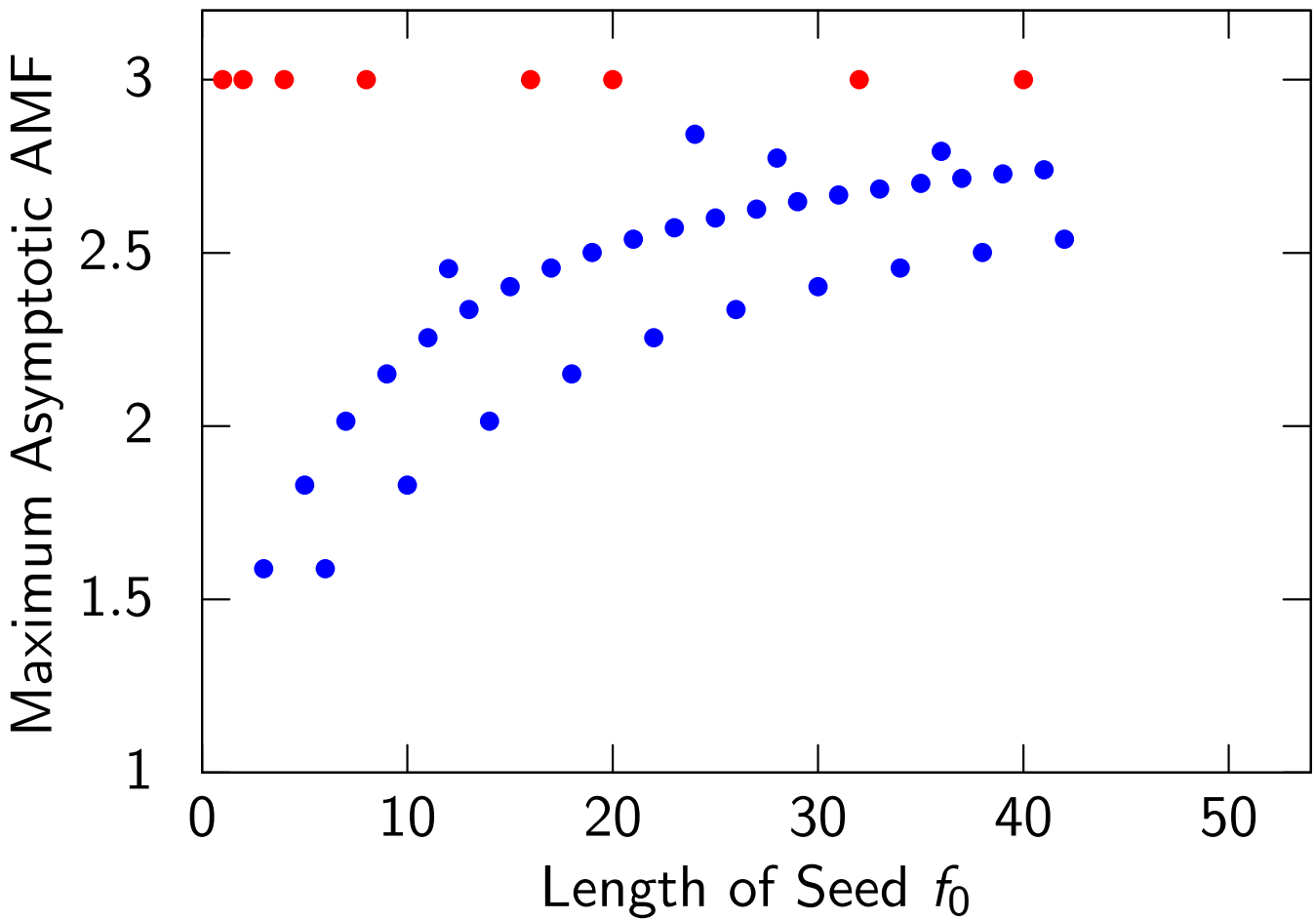
Old Result for Autocorrelation

Recall: Borwein-Mossinghoff showed that $\lim_{n\to\infty} \mathrm{AMF}(f^n) \leq 3$, with equality achievable at lengths 1, 2, 4, 8, 16, 20, 32, 40



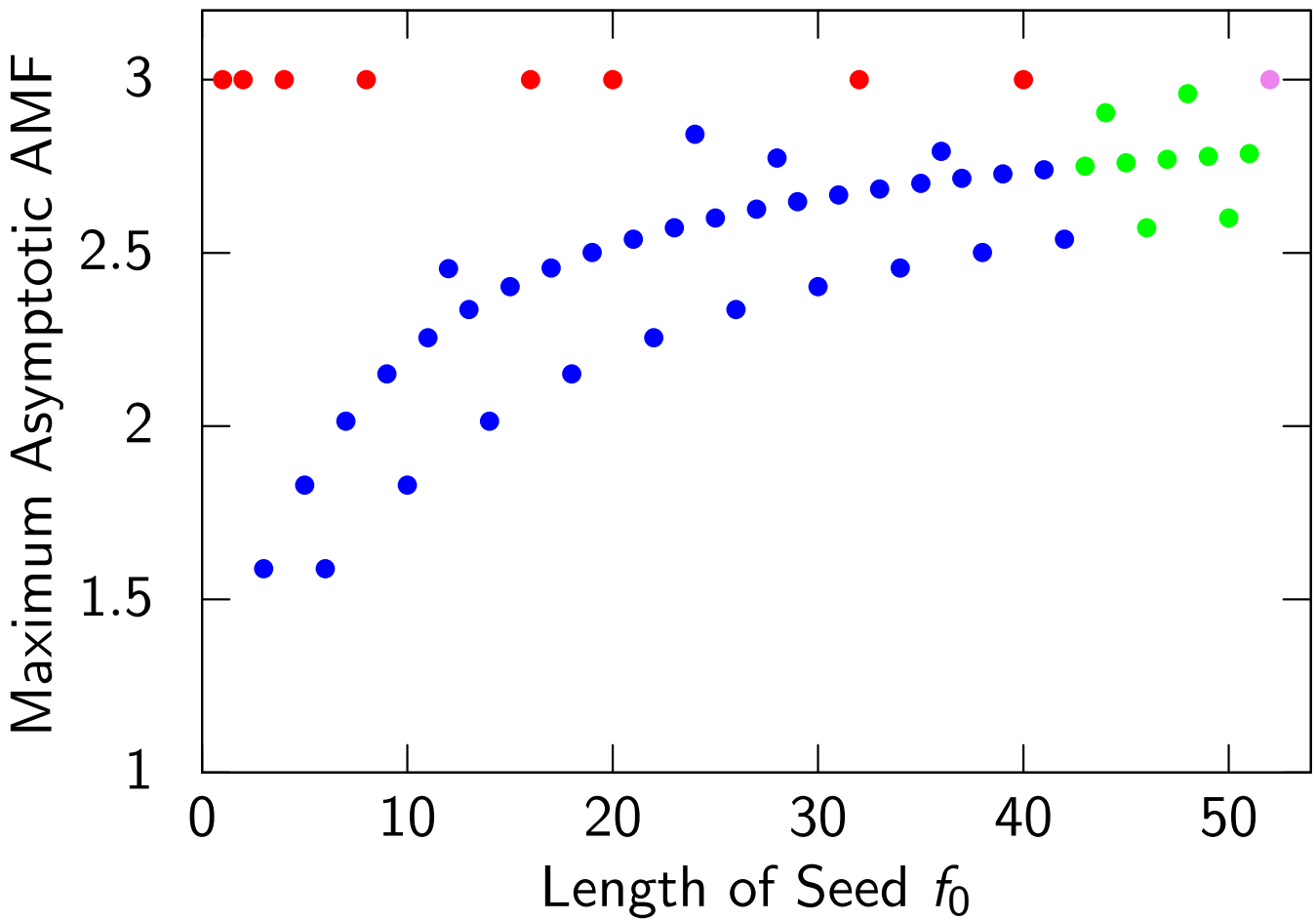
Old Result for Autocorrelation

On our own machines: highest possible $\lim_{n\to\infty} \mathrm{AMF}(f^n)$ with seeds of length ≤ 42. We confirm results of Borwein-Mossinghoff.



New Result for Autocorrelation

We used a massively parallel search using the Open Science Grid to extend the search to length 52



What is Going On?

A special type of sequence pairs called Golay complementary pairs first researched by Golay (1951) in connection with multislit spectrometry

- Golay originally constructed them for lengths 2^a
- Golay later discovered pairs of length 10, excluded various other lengths, and wondered if they might exist at length 26

The Connection

Further constructions have been discovered.

- Known to be Golay sequences of lengths $2^a 10^b 26^c$ for $a, b, c \geq 0$
- Curious: for lengths $2 \leq \ell \leq 52$, asymptotic merit factor 3 is achievable precisely when ℓ is double that of of a Golay pair

Theorem (K.-Trunov, 2017)

A seed f^0 of length > 1 gives rise to a stem $f^0, f^1, \ldots$ with $\lim_{n\to\infty} \mathrm{AMF}(f^n) = 3$ if and only if f^0 is the interleaving of a Golay complementary pair.

What about Crosscorrelation?

Recall: $\lim_{n\to\infty} \mathrm{CDF}(f^n, g^n)$ can be made arbitrarily close to 0, but at the cost of very high autocorrelation.

So better to calculate the limiting Pursley-Sarwate Criterion

$$\lim_{n\to\infty} \mathrm{PSC}(f^n, g^n) = \lim_{n\to\infty} \sqrt{\mathrm{ADF}(f^n)\mathrm{ADF}(g^n)} + \mathrm{CDF}(f^n, g^n)$$

Recall: for typical randomly selected sequence pairs with large ℓ, we expect

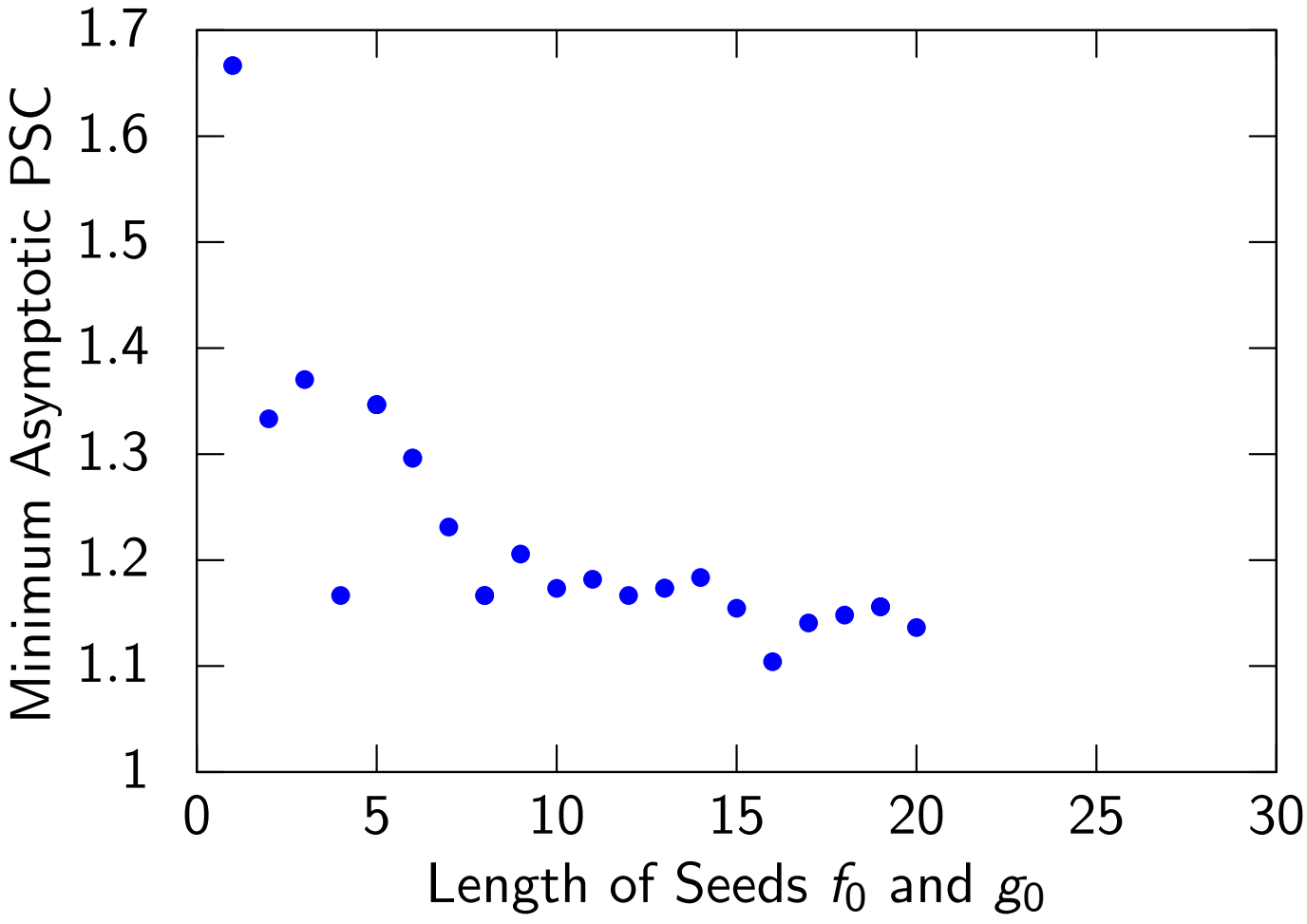
$$\mathrm{PSC}(f, g) \approx 2$$

Recall: we always have

$$\mathrm{PSC}(f, g) \geq 1$$

Crosscorrelation Result

Big Question: How close to 1 do Rudin-Shapiro-like sequences get?



Crosscorrelation Result

Big Question: How close to 1 do Rudin-Shapiro-like sequences get?