Correlation properties of signals

- Signals with excellent autocorrelation properties are useful for synchronization purposes.
- Signals with excellent crosscorrelation properties are useful for multiple-access purposes
  small
- Classes of signals include
  - Maximal length sequences (m-sequences)
  - Gold codes
  - Zadoff Chu sequences

Maximal length sequences (m-sequences)

- Maximal length shift register sequences are used in many applications including spread-spectrum systems.
- They are sometimes called pseudo-noise (PN) sequences because they seem to have noise like properties.
- They are sometimes called linear feedback shift register sequences (LFSR) because they are generated using linear feedback (mod 2).

Maximal length sequences (m-sequences)

- They are usually not used as error control codes but as signaling waveforms.
- The usefulness stems from the nice autocorrelation property m-sequences posses.
- m-sequences are similar to Fibonacci sequences except for m-sequences the arithmetic is done mod(2).
- Because of the limited number of m-sequences another class of sequences (Gold sequences) is often used.

Fibonacci sequences

$$F_n = F_{n-1} + F_{n-2}, \quad F_0 = 0,\ F_1 = 1$$

MATLAB CODE

```
clear all
F(1)=0;
F(2)=1;
for n=3:51
    F(n)=F(n-1)+F(n-2);
end
f(51)
```

n	0	1	2	3	4	5	6	7	8	9
F_n	0	1	1	2	3	5	8	13	21	34

n	10	11	12	13	14	15	16	17	18	19
F_n	55	89	144	233	377	610	987	1597	2584	4181

$F_{20} =$

Suppose the the n-th term was of the form $F_n = As^n$. Then

$$
\begin{aligned}
F_n &= F_{n-1} + F_{n-2} \\
As^n &= As^{n-1} + As^{n-2} \\
s^2 &= s^1 + 1 \\
s^2 &- s^1 - 1 = 0 \\
s &= \frac{1 \pm \sqrt{(1+4)}}{2} \\
s_0 &= \frac{1+\sqrt{5}}{2}, s_1 = \frac{1-\sqrt{5}}{2}
\end{aligned}
$$

$$F_n = As_0^n + Bs_1^n;$$

Initial Conditions $F_0 = 0,\ F_1 = 1$;

$$\begin{aligned} n = 0, &\qquad F_0 = A + B; \\ n = 1, &\qquad F_1 = As_0 + Bs_1 \\ A = \frac{F_0 s_1 - F_1}{s_1 - s_0}, &\qquad B = \frac{F_1 - F_0 s_0}{s_1 - s_0}, \end{aligned}$$

For $F_0 = 0$, $F_1 = 1$ we get the following relation

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Check this in Matlab

Fibonacci sequences

$$G_n = G_{n-1} + G_{n-2}, \quad G_0 = 1,\ G_1 = 1$$

n	0	1	2	3	4	5	6	7	8	9
G_n	1	1	2	3	5	8	13	21	34	55

n	10	11	12	13	14	15	16	17	18	19
G_n	89	144	233	377	610	987	1597	2584	4181	6765

$$G_n = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Fibonacci sequences

$$H_n = H_{n-1} + H_{n-2}, \quad H_0 = 1,\ H_1 = 2$$

n	0	1	2	3	4	5	6	7	8	9
H_n	1	2	3	5	8	13	21	34	55	89

n	10	11	12	13	14	15	16	17	18	19
H_n	144	233	377	610	987	1597	2584	4181	6765	10926

$$H_n = \left(\frac{\sqrt{5}+3}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-3}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Fibonacci sequences

Suppose $F_0 = 3$ and $F_1 = 4$. The the sequence is 3, 4, 7, 11, 18, 29, 47,... Find the general form of the Fibanacci sequence (find A and B) for this starting condition.

$$A = \underline{\hspace{6cm}}$$
$$B = \underline{\hspace{6cm}}$$

$$F_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

$$F_{20} = \underline{\hspace{6cm}}$$

Fibonacci sequences

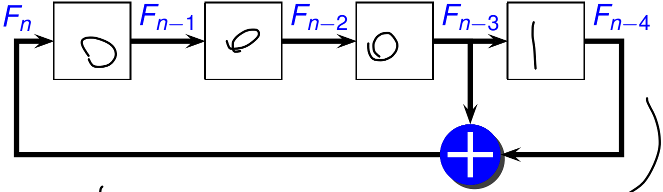
$$F_n = F_{n-3} + F_{n-4}, \quad F_0 = 0,\ F_1 = 0,\ F_2 = 0,\ F_3 = 1$$

n	0	1	2	3	4	5	6	7	8	9
F_n	0	0	0	1	0	0	1	1	0	1

n	10	11	12	13	14	15	16	17	18	19
F_n	2	1	1	3	3	2	4	6	5	6

$$\begin{aligned} F_n &= (0.1593)(1.2207)^n + (0.1187 + j0.2045)(-0.2481 + j1.0340)^n \\ &\quad + (0.1187 - j0.2045)(-0.2481 - j1.0340)^n + (-0.3967)(-0.7245)^n \end{aligned}$$

Fibonacci Sequences



shift register

1	0	0	0
0	1	0	0
0	0	1	0
1	0	0	1
1	1	0	0

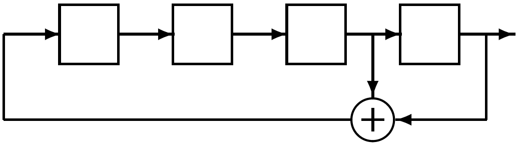
Fibonacci Sequences, mod 2

$$F_n = F_{n-3} + F_{n-4} \mod (2), \;\; F_0 = 0,\; F_1 = 0,\; F_2 = 0,\; F_3 = 1$$

n	0	1	2	3	4	5	6	7	8	9
F_n	0	0	0	1	0	0	1	1	0	1

n	10	11	12	13	14	15	16	17	18	19
F_n	0	1	1	1	1	0	0	0	1	0

Maximal length sequences (m-sequences)



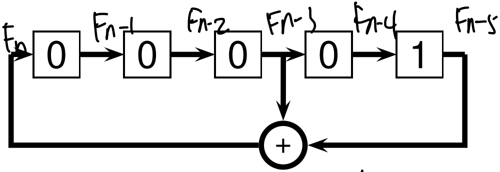
shift right.

0 0 0 1	0 1 0 1
1 0 0 0	1 0 1 0
0 1 0 0	1 1 0 1
0 0 1 0	1 1 1 0
1 0 0 1	1 1 1 1
1 1 0 0	0 1 1 1
0 1 1 0	0 0 1 1
1 0 1 1 mod 2	0 0 0 1

The output of the shift register is the periodic sequence.

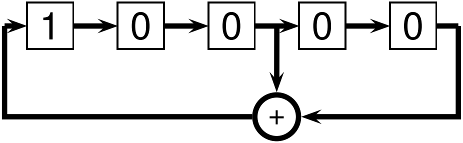
1 0 0 0 1 0 0 1 1 0 1 0 1 1 1

Maximal length sequences (m-sequences)

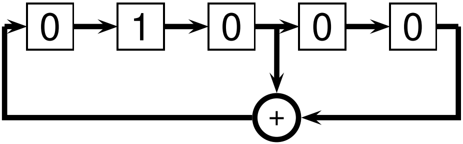


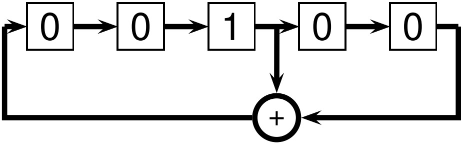
31 none

$$F_n = (F_{n-3} + F_{n-5}) \bmod 2$$

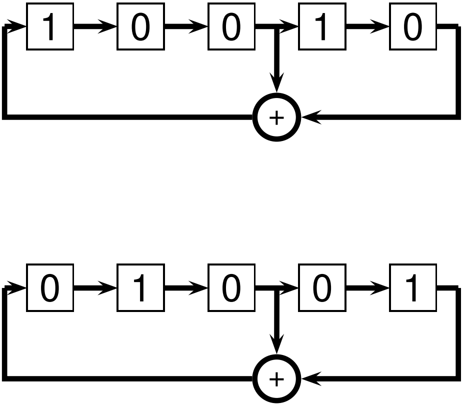


Maximal length sequences (m-sequences)

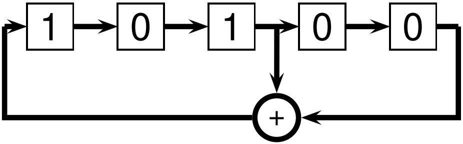


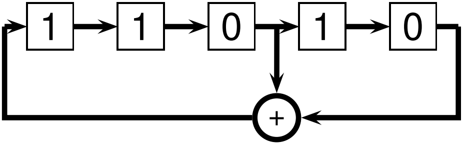


Maximal length sequences (m-sequences)



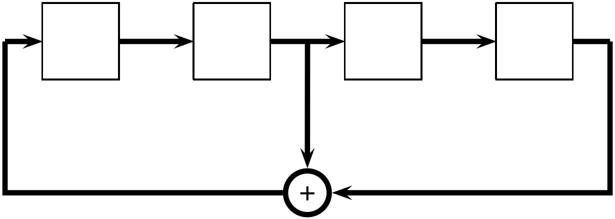
Maximal length sequences (m-sequences)





Linear Shift Register Sequences

Not all shift registers with linear feedback give a maximal length sequence. For example, the register shown below does not.



The state of the shift register is

0 0 0 1
1 0 0 0
0 1 0 0
1 0 1 0
0 1 0 1
0 0 1 0
0 0 0 1

So the sequence is of length 6 (not 15).

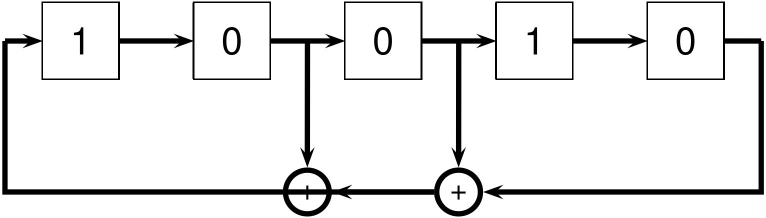
If the register is started in different states we get different sequences.

1	1	1	1
0	1	1	1
0	0	1	1
1	0	0	1
1	1	0	0
1	1	1	0
1	1	1	1

0	1	1	0
1	0	1	1
1	1	0	1
0	1	1	0

This is another sequence of length ~~6~~ 10. Another sequence is of length 3. With these three sequences we have exhausted all possible starting states except the all zero state.

Not a maximal length sequences



1 1 0 1 1

0 1 1 0 1

1 0 1 1 0

1 1 0 1 1

Unique Cycles (for non-maximal length sequence)

1	12	6	3	1	2	3	4
11111	01111	00111	11011	00000	10101	01001	00110
	10111	00011	01101		01010	00100	10011
	01011	10001	10110			10010	11001
	00101	11000					01100
	00010	11100					
	00001	01110					
	10000						
	01000						
	10100						
	11001						
	11100						
	11110						

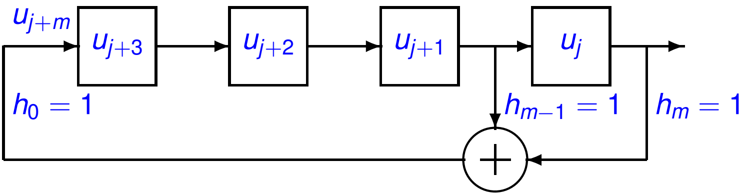
Maximal length sequences (m-sequences)

- In general the feedback connection can be described by a polynomial $h(x)$.
- Let $h(x) = h_0 x^n + h_1 x^{n-1} + \cdots + h_{n-1} x + h_n$ with $h_i \in \{0, 1\}$.
- The taps of the shift register that are fed back correspond to $h_i = 1$.
- We require $h_n = h_0 = 1$ (otherwise we could make the shift register shorter).
- The sequence at the output of the shift register can be expressed as

$$f_{j+n} = h_1 f_{j+n-1} + \cdots + h_{n-1} f_{j+1} + h_n f_j$$

as can be seen below.

Maximal length sequences (m-sequences)



Properties of m-sequences

- The period of the sequence is denoted by N. $= 2^m - 1$
- If the length of the shift register is m the longest period possible for the sequence is $2^m - 1$.
- This is because the shift register could be in one of 2^m states.
- However, the all zero state would only generate the all zero sequence.
- Thus a nonzero sequence could correspond to the shift register going through all the $2^m - 1$ nonzero states before repeating.

2^{m-1} 1's

$2^{m-1} - 1$ 0's

Properties of m-sequences

$2^{m-1} = \#$ ones

$2^{m-1} - 1 = \#$ zeros

1. The sequence length is $2^m - 1$. This is because the shift register can cycle through all nonzero states before repeating. The number of nonzero states is 2^{m-1}.
2. The number of ones in the sequence is 2^{m-1} and the number of zeros is $2^{m-1} - 1$. This is because the states are all possible length m binary vectors except the all zero vector. Including the all zero vector would yield an equal number of 0's and 1's. Not including the all zero vector decreases the number of 0's by 1.

Properties of m-sequences

3. (Shift and Add) The sum of any two (distinct) shifts of a single m-sequence is a different shift of the same sequence. To see this, consider a sequence out of the shift register with initial state $a_1, ..., a_n$. The sequence generated is

$$\begin{aligned} a_{n+1} &= h_1 a_n + \cdots + h_{n-1} a_2 + h_n a_1 \\ a_{n+j} &= h_1 a_{j+n-1} + \cdots + h_{n-1} a_{j+1} + h_n a_j. \end{aligned}$$

Consider another sequence started in a different initial state $b_1, ..., b_n$. The sequence generated is

$$\begin{aligned} b_{n+1} &= h_1 b_n + \cdots + h_{n-1} b_2 + h_n b_1 \\ b_{n+j} &= h_1 b_{j+n-1} + \cdots + h_{n-1} b_{j+1} + h_n b_j. \end{aligned}$$

The mod 2 sum of these two sequences is $c_{j+n} = a_{j+n} + b_{j+n}$ and is exactly the sequence from the same shift register by starting in state $a_1 + b_1, ..., a_n + b_n$ where the addition is mod 2.

Shift and Add Property: Example 1

$$\underline{100010011010111}100010011010111$$

$$\oplus \quad 1\underline{100010011010111}10001001101011$$

$$0100110101111\underline{000100110101111}00$$

Shift and Add Property: Example 2

$$
\begin{array}{rl}
 & 100010011010111100010011010111 \\
\oplus & 111000100110101111000100110101 \\
\hline
 & 011010111100010011010111100010
\end{array}
$$

Shift and Add Property: Example 3

$$
\begin{array}{rl}
 & \underline{100010011010111}100010011010111 \\
\oplus & 111\underline{100010011010111}100010011010 \\
\hline
 & 0111\underline{100010011010111}10001001101
\end{array}
$$

Shift and Add Property: Example 4

100010011010111100010011010111

110001001101011110001001101011

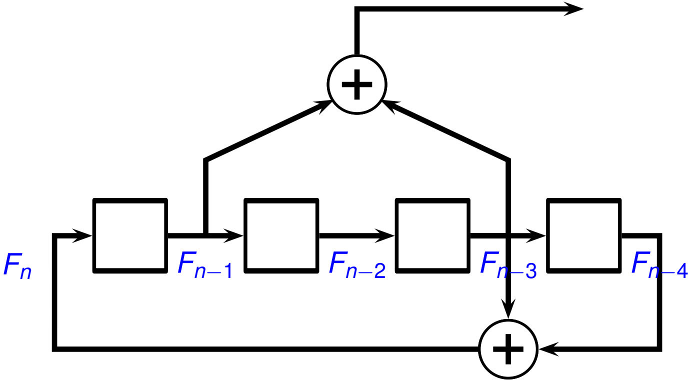
$\oplus$ 111000100110101111000100110101

101011110001001101011110001001

Shift and Add Property: Example 5

$$
\begin{array}{rl}
 & \underline{100010011010111}100010011010111 \\
\oplus & 010111\underline{100010011010111}100010011 \\
\hline
 & 11010111\underline{100010011010111}1000100
\end{array}
$$

Shift and Add Property



Shift and add property

- For example take the shift register of length 4 shown earlier that produces a sequence of length 15.
- One sequence out of the shift register is found by starting in state 0001. The sequence is 100010011010111 and then repeats.
- Another sequence is found by starting in state 1011 and is 110101111000100 and then repeats.
- If these two sequences are added mod 2 we get a third sequence.

$$\begin{array}{r} 100010011010111 \\ \oplus\ 110101111000100 \\ \hline 010111100010011 \end{array}$$

- This sequence can be generated from the same shift register by starting in state 1010 (which is the mod-2 sum of the two starting states).

Shift and add property

mod 2

		$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

		$\times$
+1	+1	1
+1	-1	-1
-1	+1	-1
-1	-1	1

Equivalently if the two sequences are converted to ± 1 by the mapping $0 \to 1,\ 1 \to -1$ and then multiplied we get a third sequence.

	-1	+1	+1	+1	-1	+1	+1	-1	-1	+1	-1	+1	-1	-1	-1
$\times$	-1	-1	+1	-1	+1	-1	-1	-1	-1	+1	+1	+1	-1	+1	+1
	1	-1	1	-1	-1	-1	-1	1	1	1	-1	1	1	-1	-1

Properties of m-sequences

most important

$0 \rightarrow 1$
$1 \rightarrow -1$

$u_i \in \{0,1\}$,

自相关

4. The (periodic) autocorrelation function of the ± 1 sequence obtained by the transformation $v_j = (-1)^{u_j}$ is two valued. That is

$$\theta_v(l) = \sum_{i=0}^{N-1} v_i \underline{v_{i+l}} = \begin{cases} N, & l = 0 \bmod (N) \\ -1, & l \neq 0 \bmod (N) \end{cases}$$

This is obvious if $l = 0$ for then $v_i v_{i+l} = 1$ so the sum is N.

U_i	V_i
0	+1
1	-1

mod N

$V_n = V_0 \quad V_{n+1} = V_1$

Properties of m-sequences

$u_i \in \{0, 1\}$

- If $l \neq 0$ then the result is obtained by realizing that

$$v_i v_{i+l} = (-1)^{u_i}(-1)^{u_{i+l}} = (-1)^{u_i + u_{i+l}}.$$

- Clearly the sum $(u_i + u_{i+l})$ on the right matters only mod 2.
- Since $l \neq 0$, $u_i + u_{i+l} = u_{i+k}$ for some integer k. This is using the shift and add property.
- So for $l \neq 0$

$$\theta_v(l) = \sum_{i=0}^{N-1} (-1)^{u_{i+k}} = 2^{m-1}(-1) + (2^{m-1} - 1)(1) = -1.$$

For example consider the sequence 100010011010111 from the first shift register. Consider transforming it to a ± 1 sequence. Consider a cyclic shift of this sequence. Shift the sequence by 5 to the left (or 10 to the right).

OriginalSequence	-1	$+1$	$+1$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	$+1$	-1	-1	-1
ShiftedSequence	$+1$	$+1$	-1	-1	$+1$	-1	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$	-1
Product	-1	-1	-1	-1	$+1$	$+1$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	$+1$

- Now clearly the result of taking a sequence in the ± 1 domain and multiplying by a shifted version of that sequence is yet another shifted version of the same sequence.
- The number of zeros and ones in the original sequence correspond to the number of ones and minus ones in the ± 1 domain. When we add all the elements of this ± 1 sequence all the ones will cancel all but one of the minus ones we end up with -1 for the autocorrelation.

- Suppose

T_c - chip duration

$$s(t) = \sum_{n=0}^{N-1} a_n p_{T_c}(t - nT_c)$$

where $T = nT_c$ and $a_n \in \{+1, -1\}$.

- Suppose that this signal is sent repeatedly

$$r(t) = \sum_{m} s(t - mT).$$

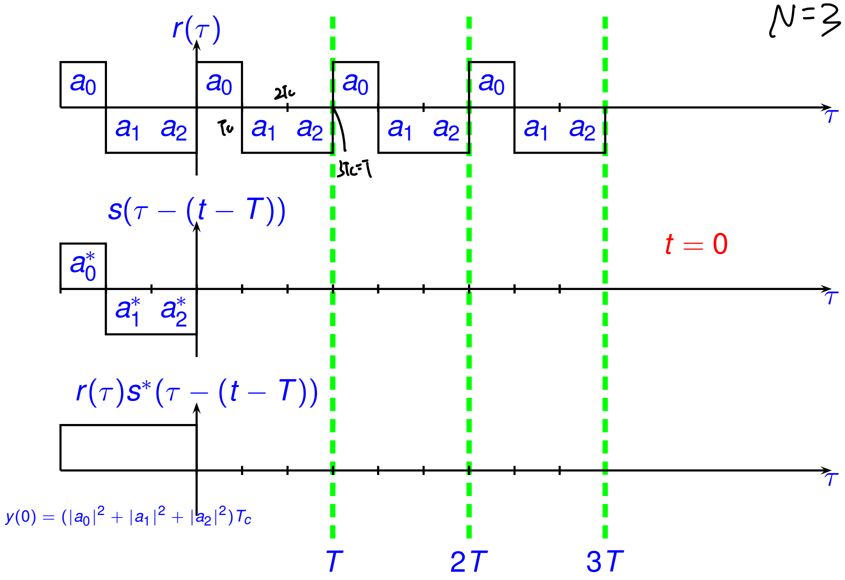
- Note that $s(t) = 0$ if $t \notin [0, T]$.
- The received signal $r(t)$ is filtered by $h(t) = s^*(T - t)$, that is, a matched filter.

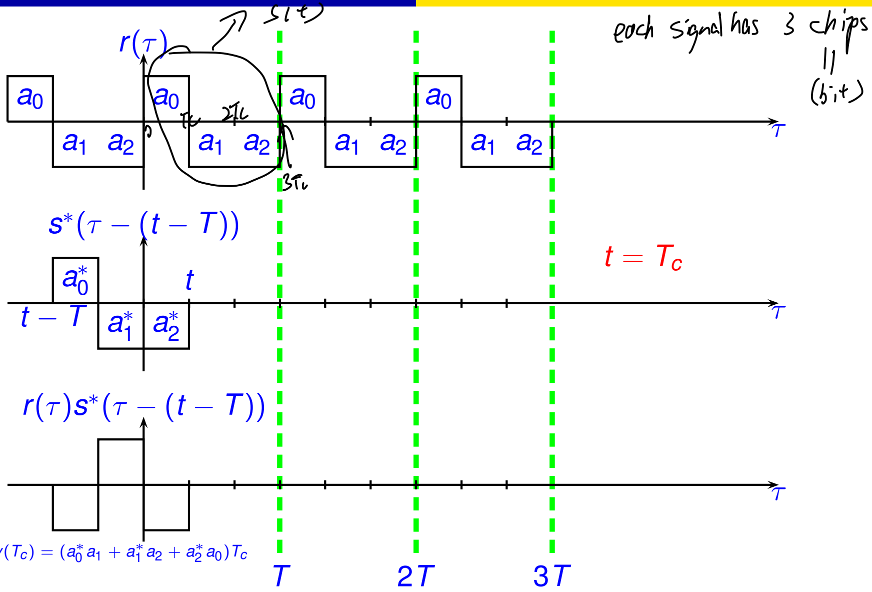
- The output of the matched filter is

$$\begin{aligned} y(t) &= \int h(t-\tau)r(\tau)d\tau \\ &= \int s^*(T-(t-\tau))r(\tau)d\tau \\ &= \int_{\tau=t-T}^{t} s^*(\tau-(t-T))r(\tau)d\tau \end{aligned}$$

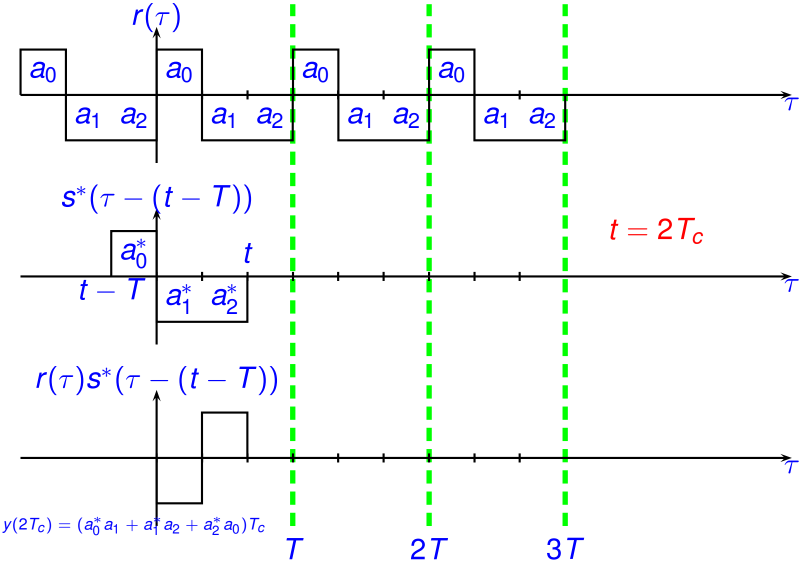
- Consider the case that $t = T = NT_c$. In this case for $0 \leq \tau \leq T$, $r(\tau) = s(\tau)$.

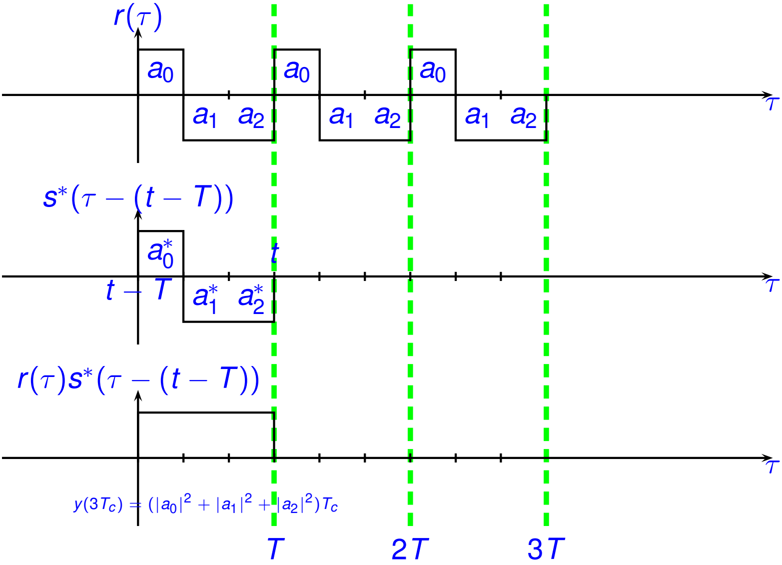
$$\begin{aligned} y(T) &= \int_{\tau=0}^{T} s^*(\tau)r(\tau)d\tau \\ &= \int_{\tau=0}^{T} |s(\tau)|^2 d\tau \\ &= \int_{\tau=0}^{T} 1 d\tau = T \end{aligned}$$


N=3
$r(\tau)$
a_0
a_1 a_2
T_c
$2T_c$
$3T_c=T$
τ
$s(\tau-(t-T))$
a_0^*
a_1^* a_2^*
$t=0$
$r(\tau)s^*(\tau-(t-T))$
$y(0)=(|a_0|^2+|a_1|^2+|a_2|^2)T_c$
T
$2T$
$3T$

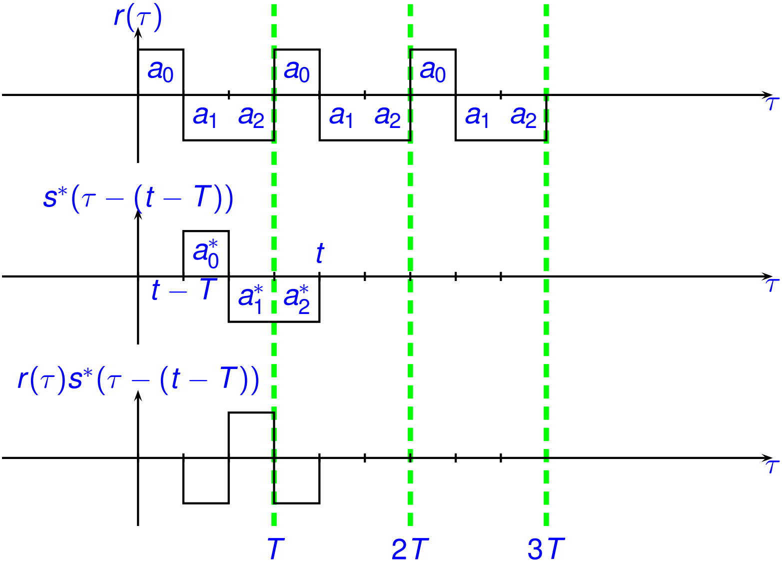


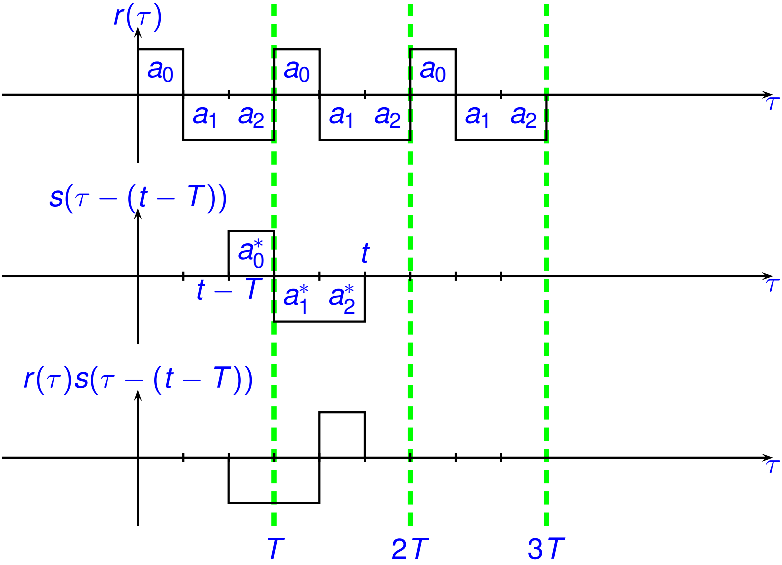
$y(T_c) = (a_0^* a_1 + a_1^* a_2 + a_2^* a_0)T_c$


$r(\tau)$
a_0 a_1 a_2
τ
$s^*(\tau - (t - T))$
a_0^* a_1^* a_2^*
t
$t - T$
$t = 2T_c$
$r(\tau)s^*(\tau - (t - T))$
$y(2T_c) = (a_0^* a_1 + a_1^* a_2 + a_2^* a_0)T_c$
T
$2T$
$3T$

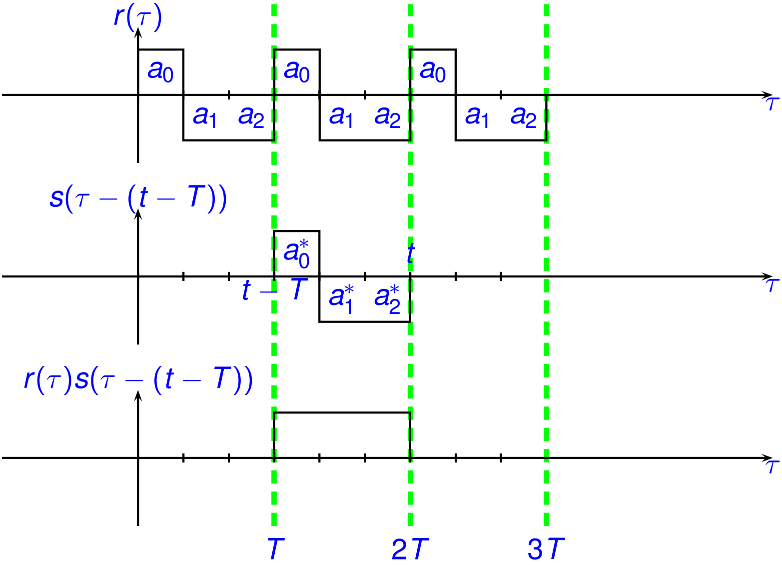


$r(\tau)$
a_0
a_1 a_2
τ
$s^*(\tau-(t-T))$
a_0^*
t
$t-T$
a_1^* a_2^*
$r(\tau)s^*(\tau-(t-T))$
$y(3T_c) = (|a_0|^2 + |a_1|^2 + |a_2|^2)T_c$
T
$2T$
$3T$

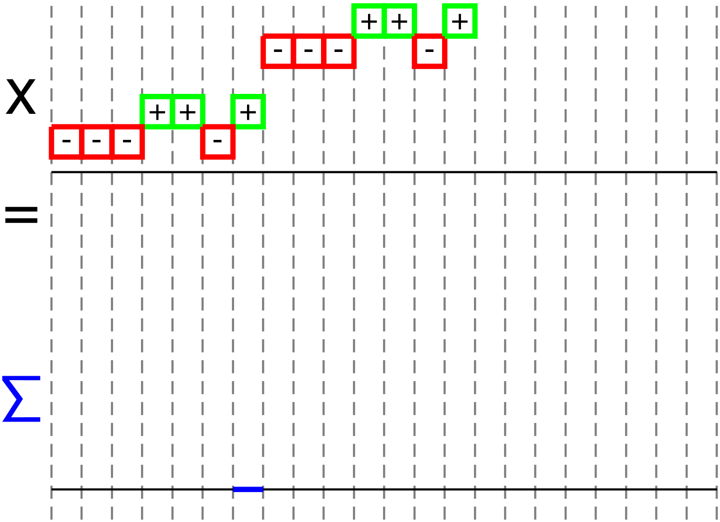

$r(\tau)$
a_0
a_1 a_2
a_0
a_1 a_2
a_0
a_1 a_2
τ
$s^*(\tau-(t-T))$
a_0^*
t
$t-T$
a_1^* a_2^*
τ
$r(\tau)s^*(\tau-(t-T))$
τ
T
$2T$
$3T$



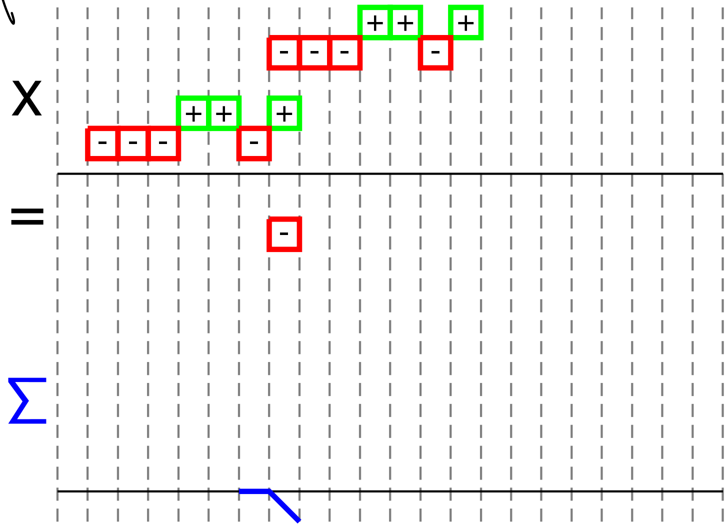
$r(\tau)$
a_0
a_1
a_2
a_0
a_1
a_2
a_0
a_1
a_2
τ
$s(\tau-(t-T))$
a_0^*
$t-T$
a_1^*
a_2^*
t
τ
$r(\tau)s(\tau-(t-T))$
τ
T
$2T$
$3T$

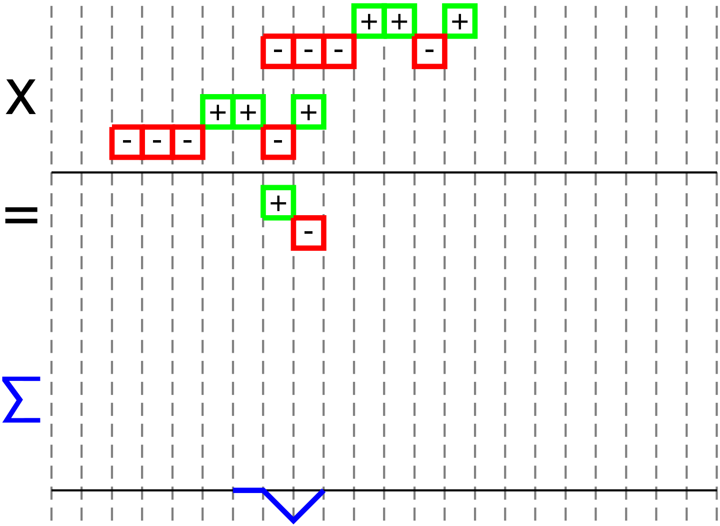

$r(\tau)$
a_0
a_1 a_2
a_0
a_1 a_2
a_0
a_1 a_2
τ
$s(\tau-(t-T))$
a_0^*
t
$t-T$
a_1^* a_2^*
τ
$r(\tau)s(\tau-(t-T))$
τ
T
$2T$
$3T$

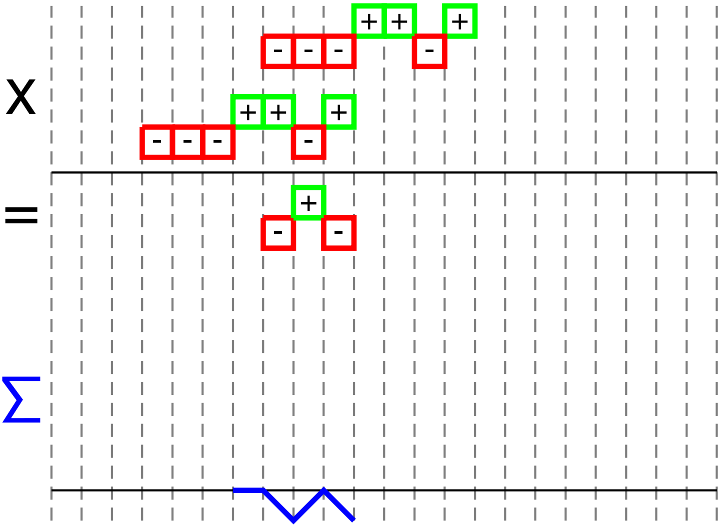
Aperiodic Autocorrelation

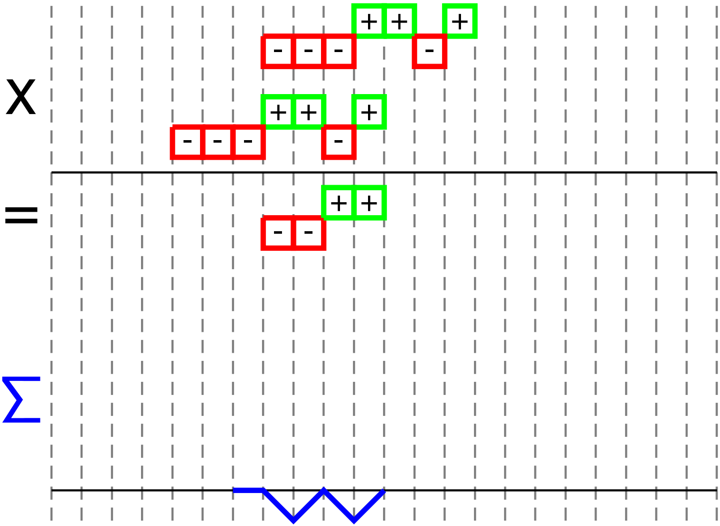

X
- - - + + - +
- - - + + - +
=
Σ

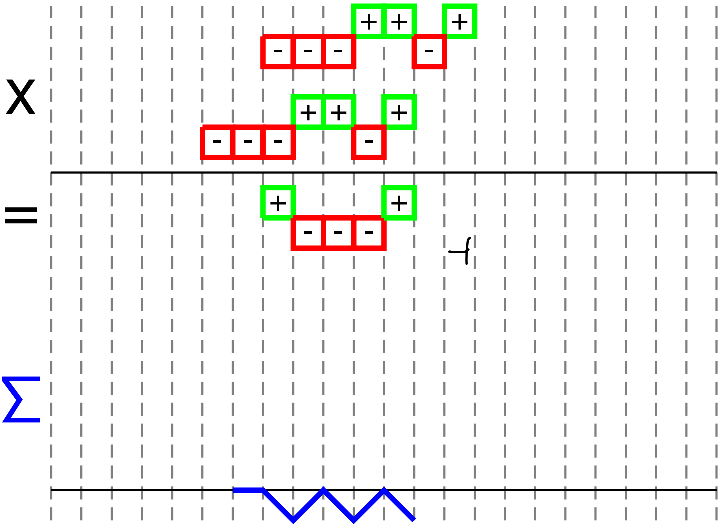
Shift one right

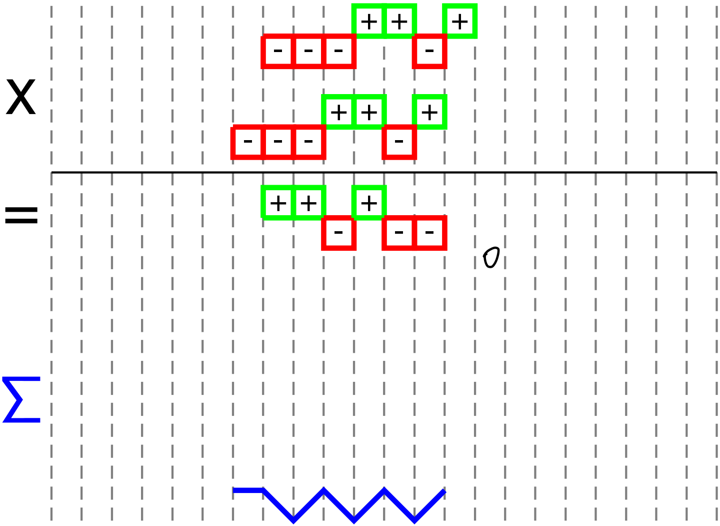


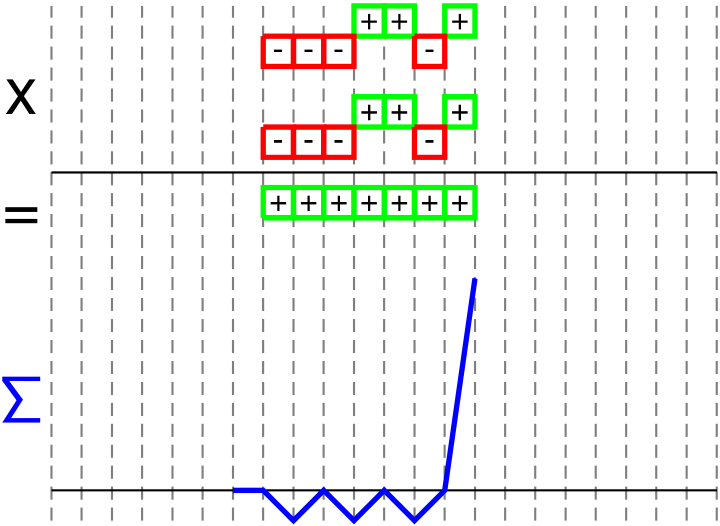

X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
+
-
Σ

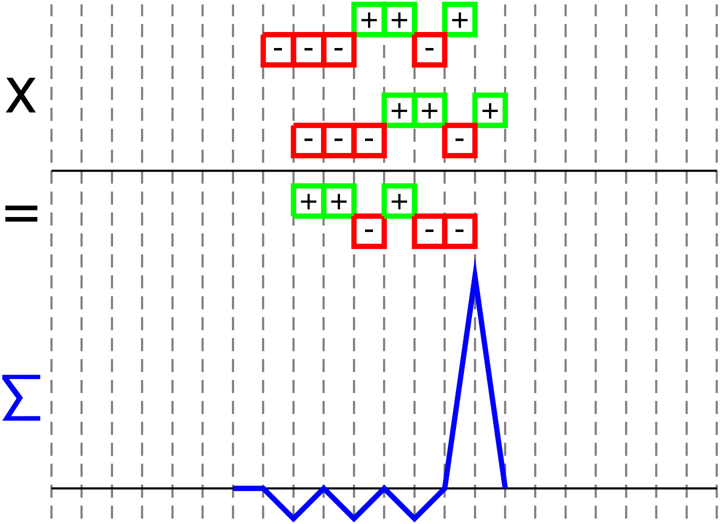

X
+
-
=
Σ

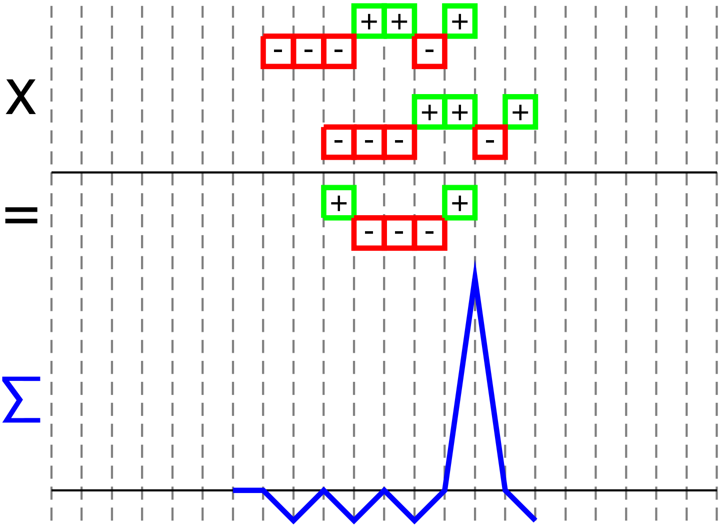

+ + +
- - - -
X
+ + +
- - - -
=
+ +
- -
∑

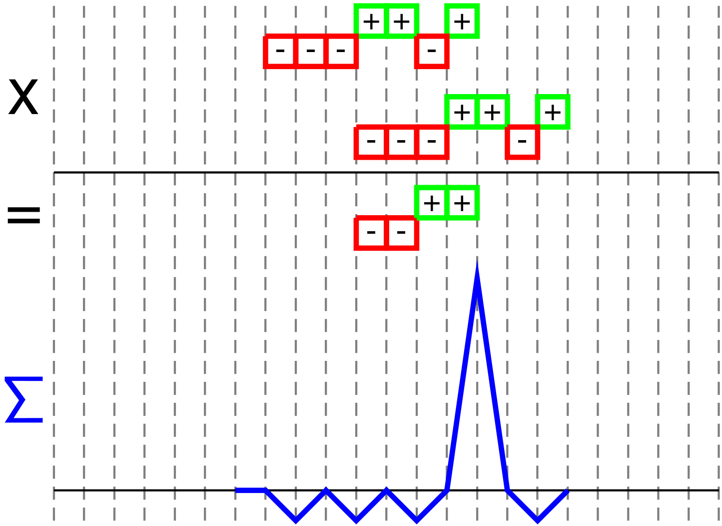

X
+ + +
- - - -
+ + +
- - - -
=
+ +
- - -
$\sum$

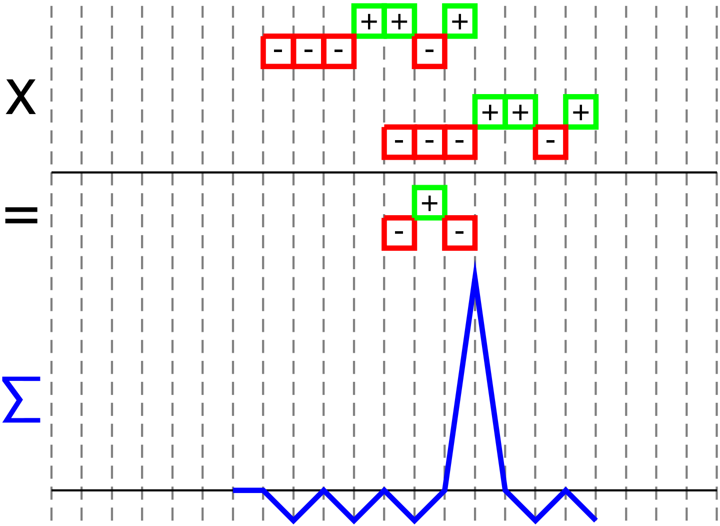

X
=
Σ
+
-
0

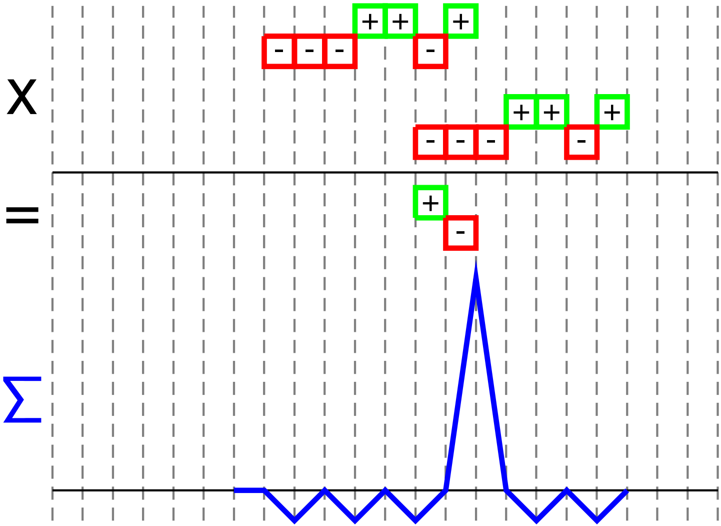

X
=
Σ
+
-


X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
+
+
+
-
-
-
Σ

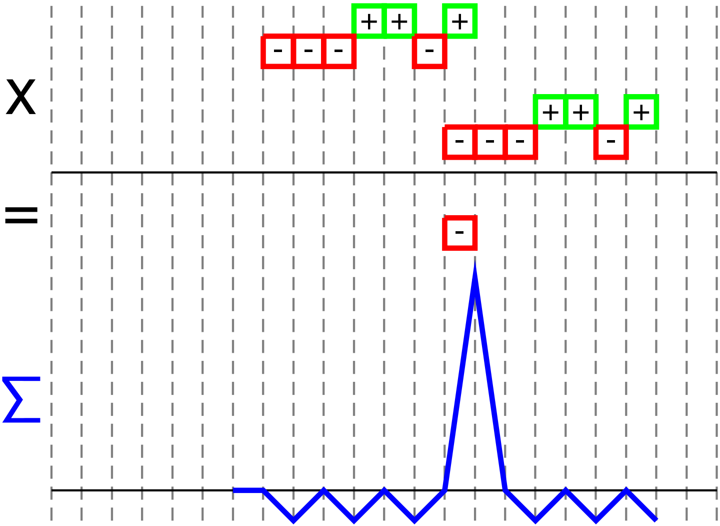

X
+ + +
- - - -
+ + +
- - - -
=
+ +
- - -
Σ

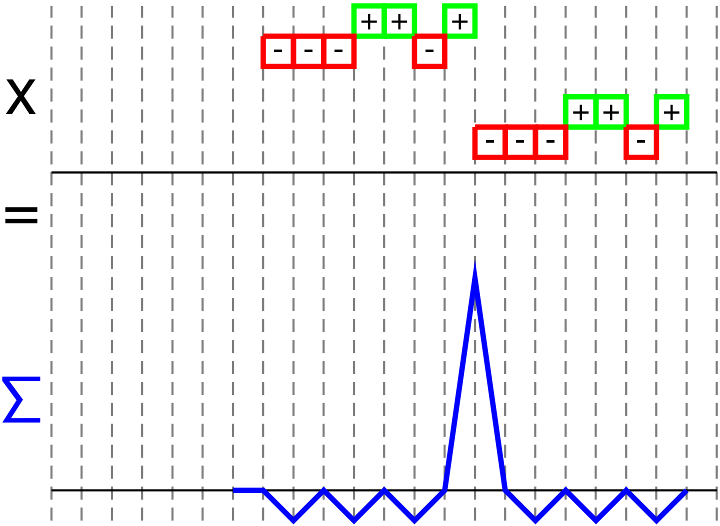

X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
+
+
-
-
Σ


X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
+
-
-
Σ

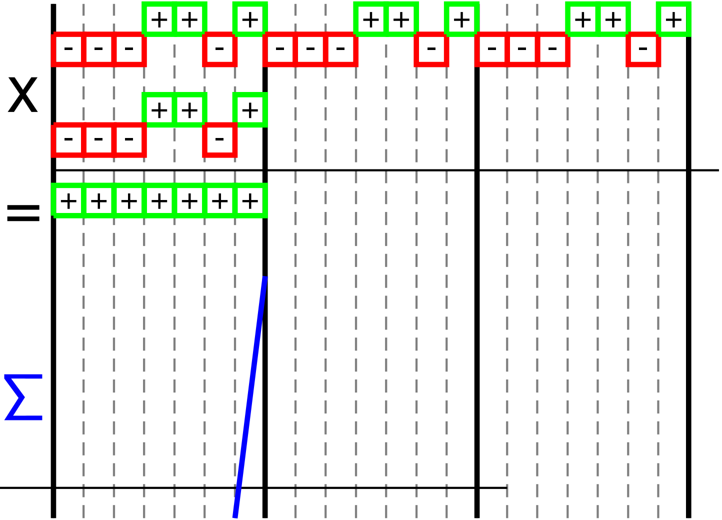


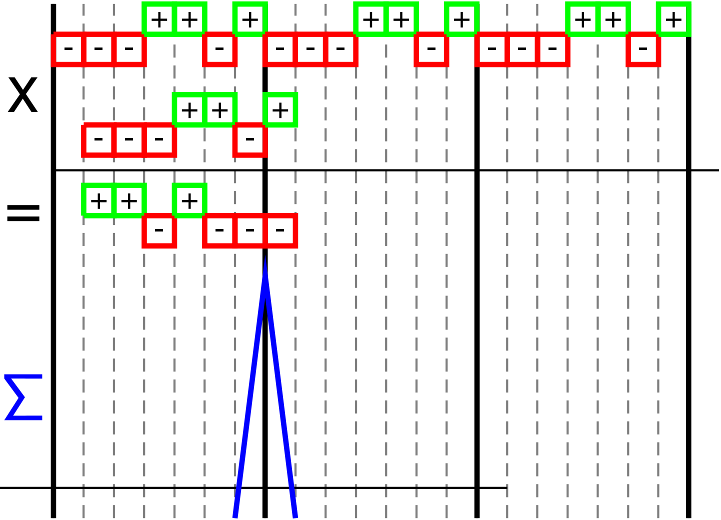
X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
+
-
Σ

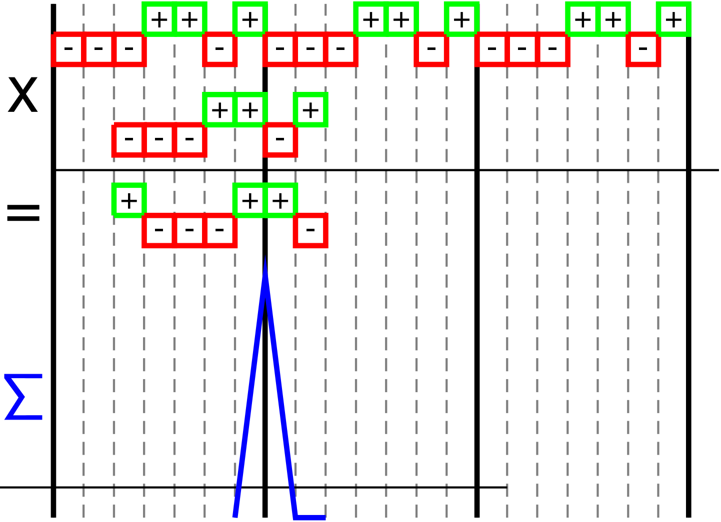

X
+
+
+
-
-
-
-
+
+
+
-
-
-
-
=
-
Σ

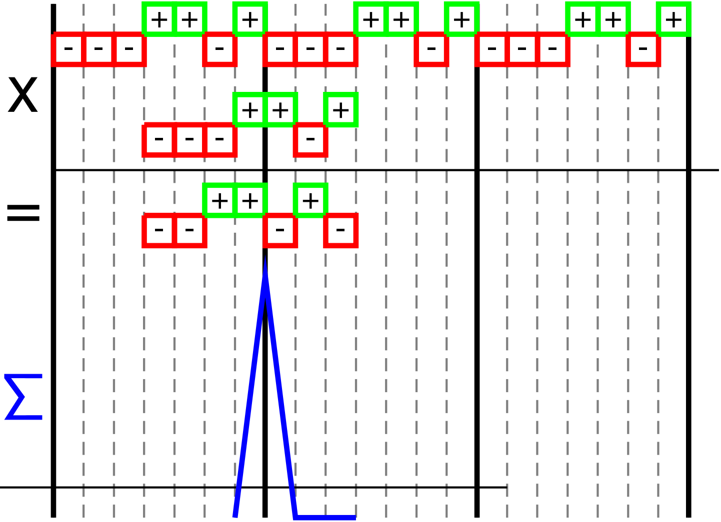

X
=
Σ
- - - + + - +
- - - + + - +

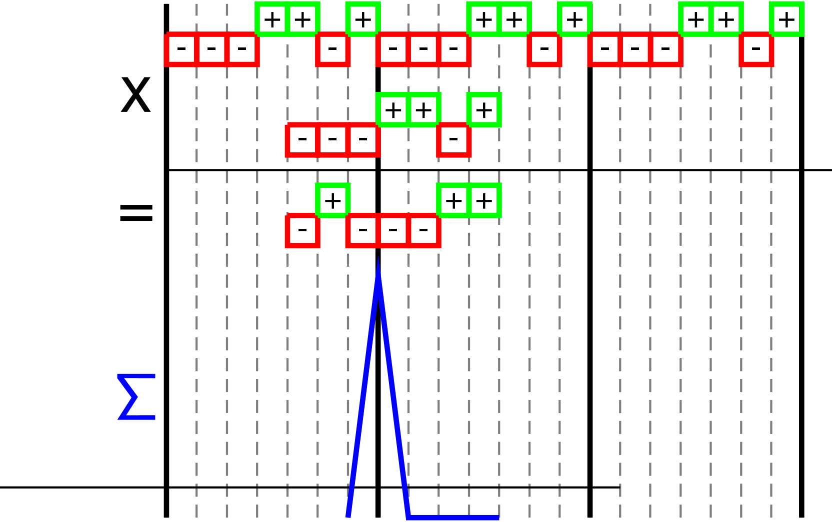
Periodic Autocorrelation

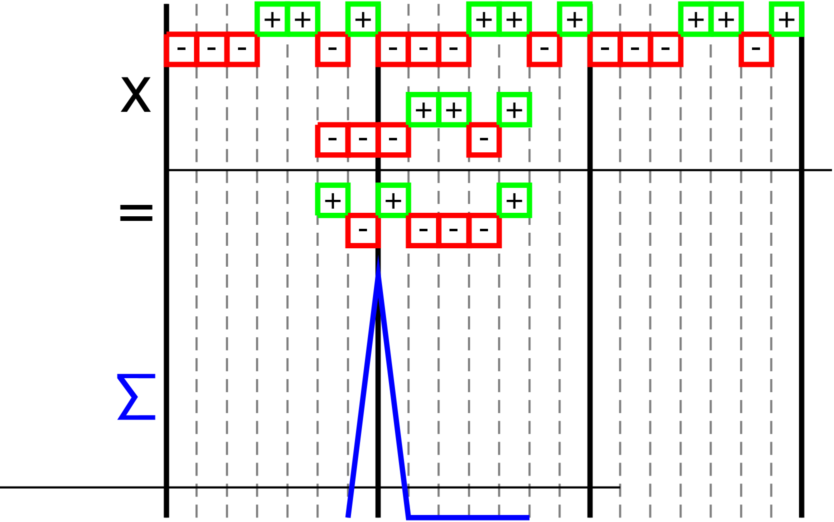

X
+ + +
- - - -
+ + +
- - - -
=
+ + + + + + +
∑

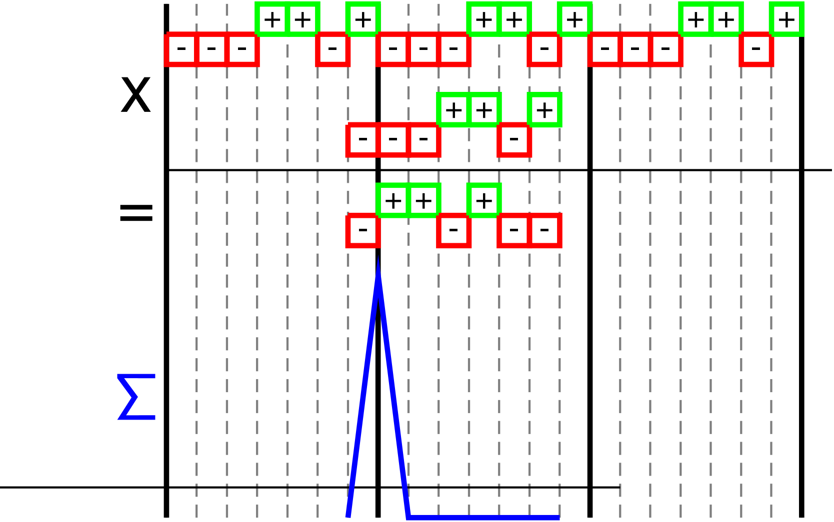

x
=
Σ
+
-

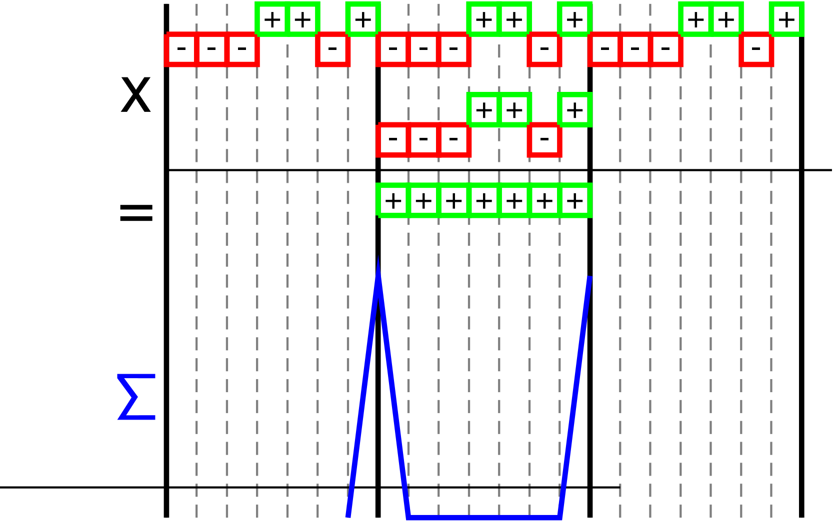

X
=
Σ

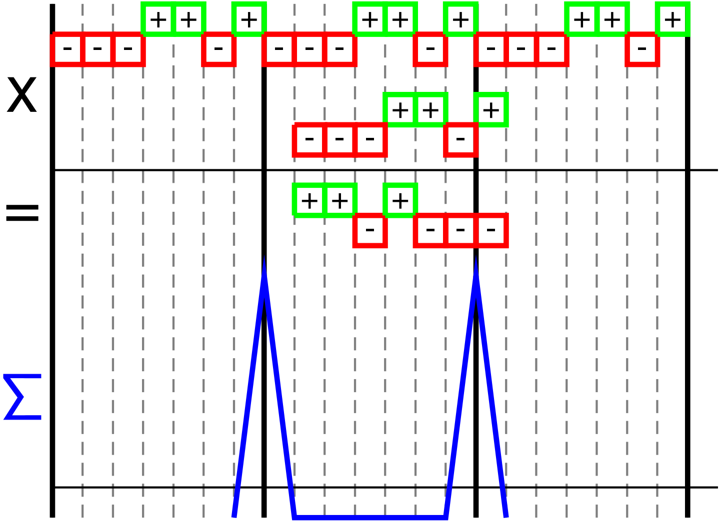

+ + + + + + + + +
- - - - - - - - - - - -
X
+ + +
- - - -
=
+ + +
- - - -
Σ

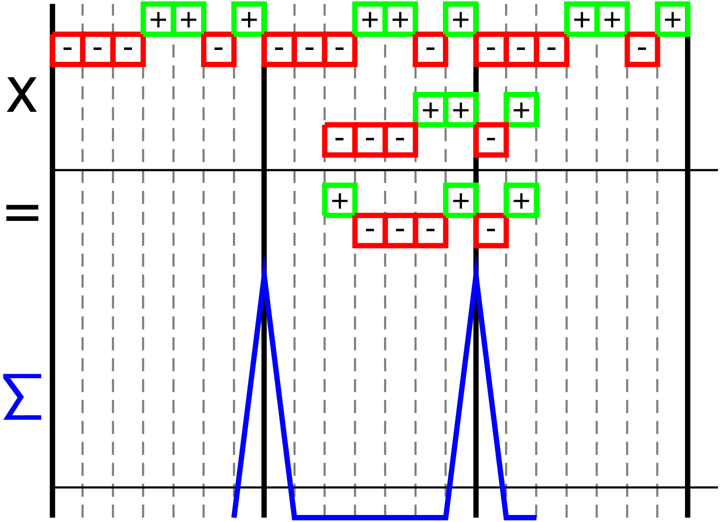

X
=
Σ


X
=
Σ

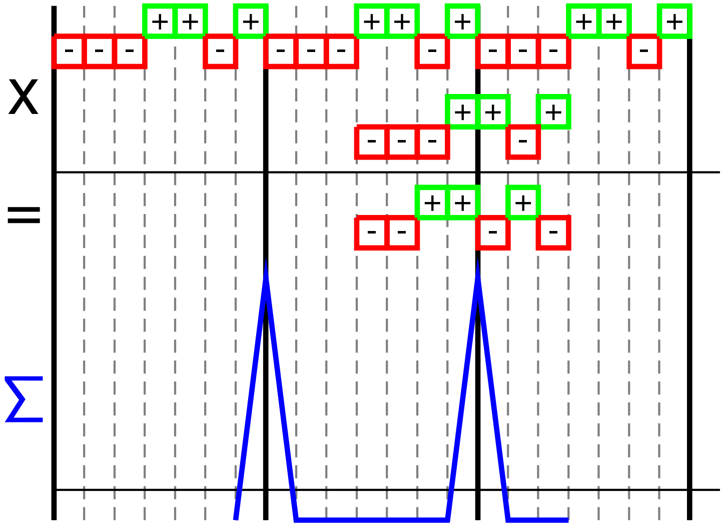

X
=
Σ

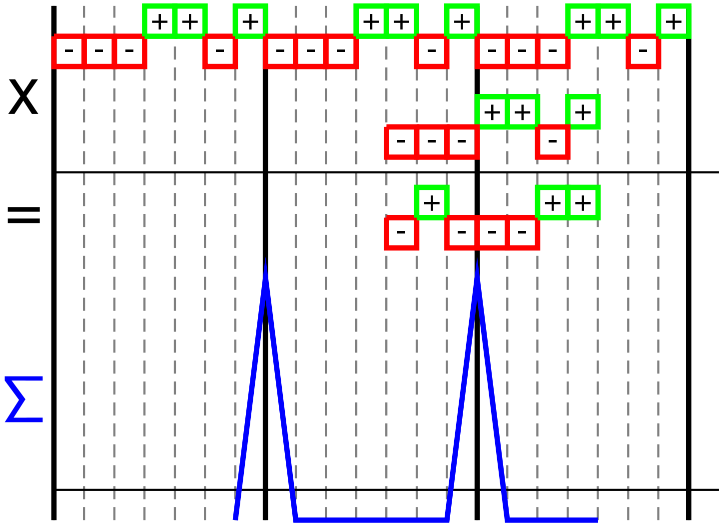

X
=
Σ

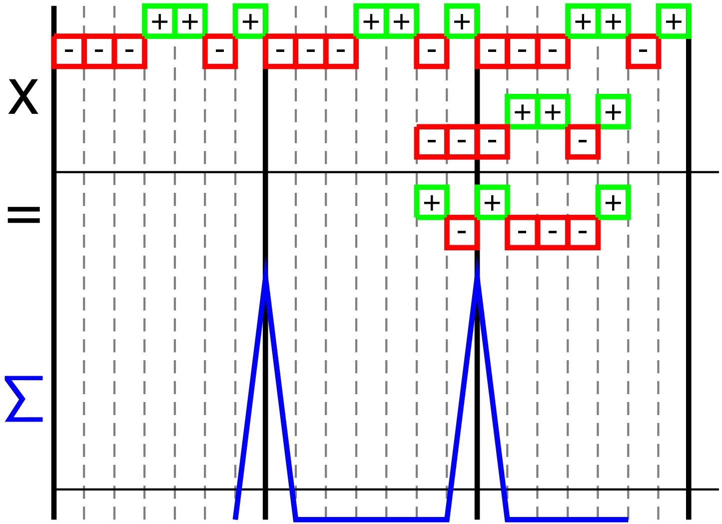

X
=
Σ

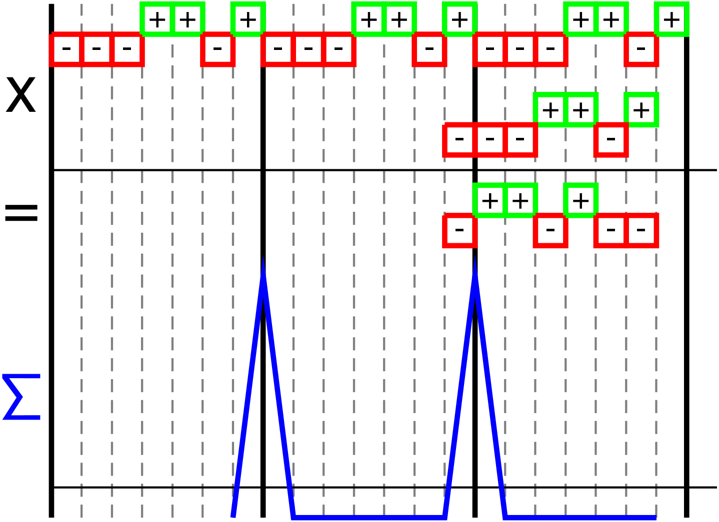


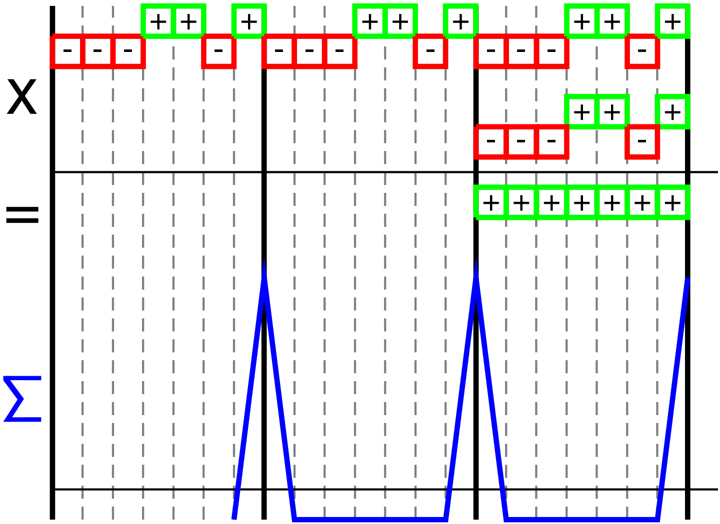
X
=
Σ


X
=
Σ


X
=
Σ
+ + + + + + + + +
- - - - - - - - - - - - -
+ + +
- - - -
+ + +
- - - -

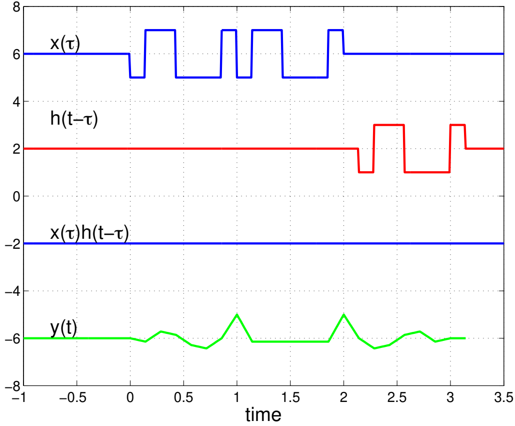

x
+ + + + + + + + + + + + + +
- - - - - - - - - - - - - - - -
=
Σ


+ + + + + + + + +
- - - - - - - - - - - - -
X
+ + +
- - - -
=
+ + +
- - - -
∑

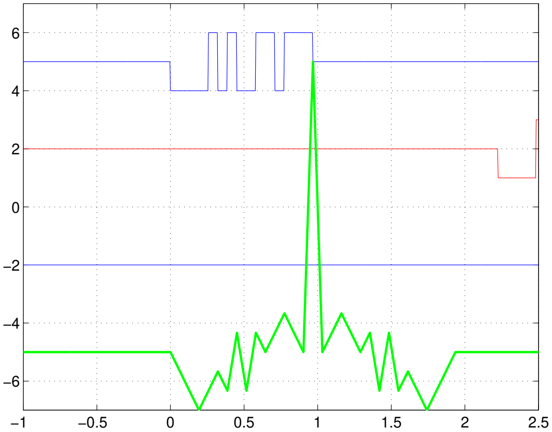


X
=
Σ

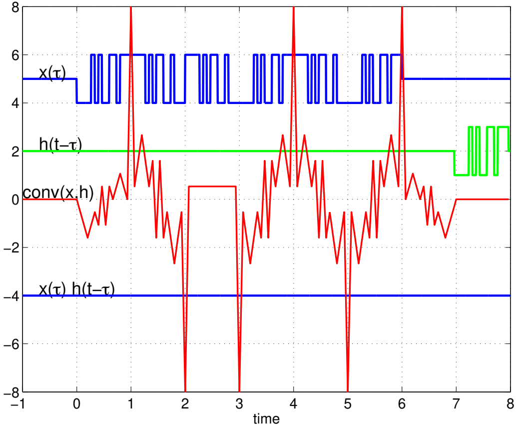
Filter output for a length 7 sequence



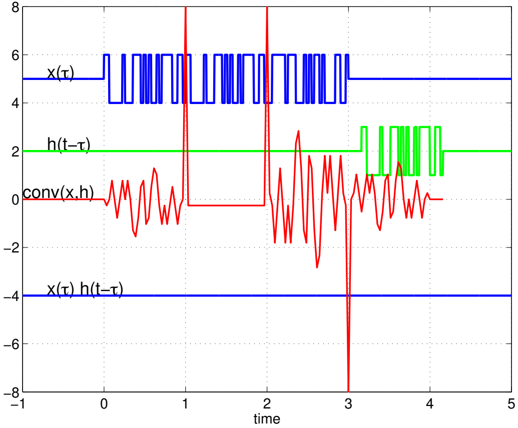
Filter output for a length 15 sequence



Filter output for a length 15 sequence



Filter output for a length 31 sequence

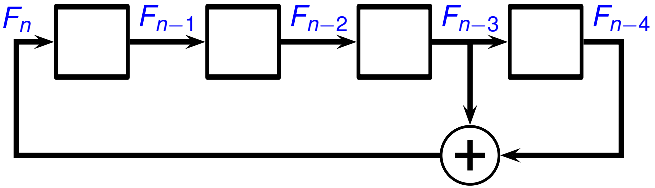


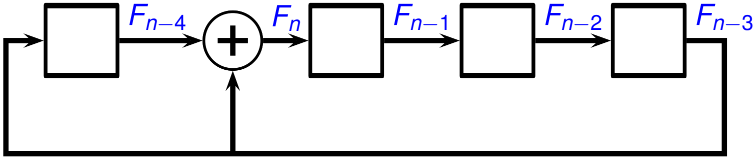
Properties of m-sequences

5. The number of distinct m-sequences is of length $2^n - 1$ is $\phi(2^m - 1)/m$ where $\phi(x)$ is Euler phi-function (also called totient function) $\phi(L)$ is the number of positive integers less than or equal to L that are relatively prime (greatest common divisor is 1) to L.

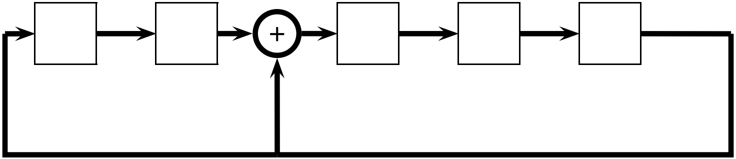
m	$2^m - 1$	Number of Sequences
2	3	1
3	7	2
4	15	2
5	31	6
6	63	6
7	127	18
8	255	16
9	511	48
10	1023	60

Fibonacci vs. Galois Implementation





Galois Implementation of maximal length sequences (m-sequences)

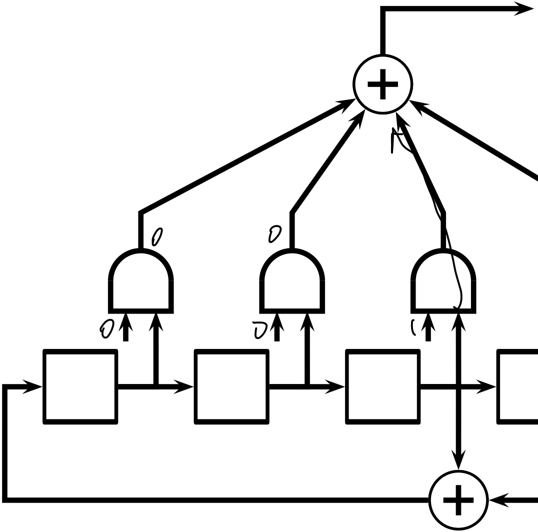


0 0 0 0 1	1 1 1 1 1	1 1 1 0 1
1 0 1 0 0	1 1 0 1 1	1 1 0 1 0
0 1 0 1 0	1 1 0 0 1	0 1 1 0 1
0 0 1 0 1	1 1 0 0 0	1 0 0 1 0
1 0 1 1 0	0 1 1 0 0	0 1 0 0 1
0 1 0 1 1	0 0 1 1 0	1 0 0 0 0
1 0 0 0 1	0 0 0 1 1	0 1 0 0 0
1 1 1 0 0	1 0 1 0 1	0 0 1 0 0
0 1 1 1 0	1 1 1 1 0	0 0 0 1 0
0 0 1 1 1	0 1 1 1 1	0 0 0 0 1
1 0 1 1 1	1 0 0 1 1	

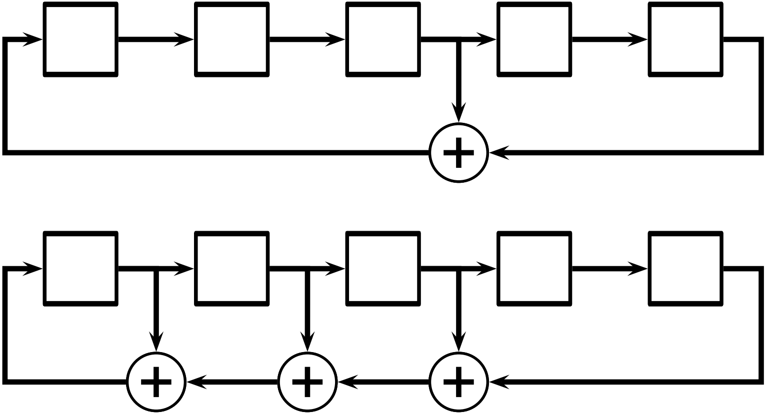
Alternative Maximal length sequences (m-sequences)

- The alternative (Galois) implementation produces the same sequence as the pure feedback form if the feedback connections are reciprocal.
- This implementation avoids doing a large number of mod 2 additions that might have longer propagation delay of the previous (Fibonacci) implementation.

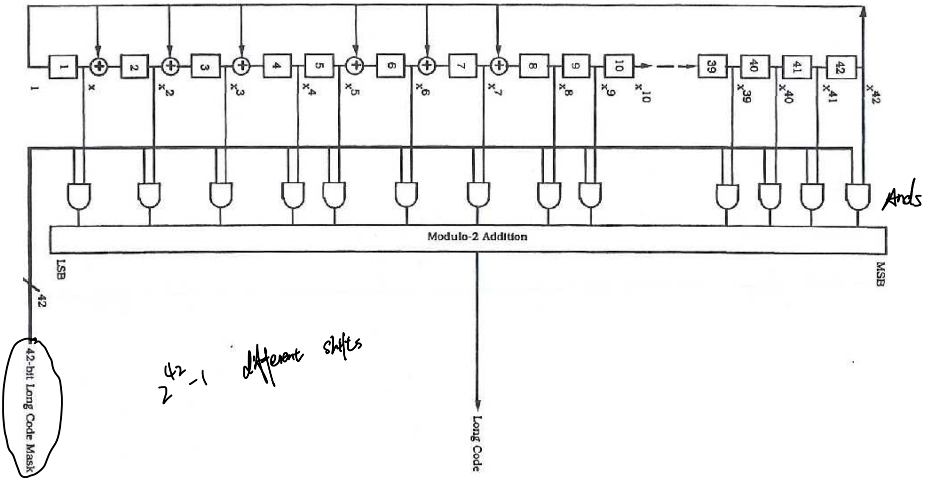
Masking for different m-sequences



Distinct m-sequences



IS-95 Implementation of Long Code for 2G Cellular



Waveform Autocorrelation

Below we show a waveform consisting of a sequence of pulses of amplitude ± 1 determined from an m-sequence and the continuous time autocorrelation function

$$\hat{s}(\tau) = \int_{-\infty}^{\infty} s(t)s(t-\tau)dt.$$

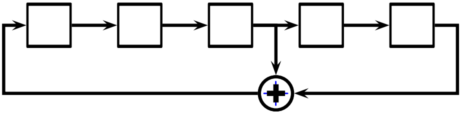
It should be noted that the continuous time autocorrelation function defined above is the same as the discrete periodic correlation when the argument τ of the continuous correlation function is an integer multiple of the duration of a single bit. In between the autocorrelation function varies linearly.

Problem with m-sequences

- The problem with m-sequences is that there are not enough distinct m-sequences to accommodate many users.
- Distinct means that the m-sequences are not just cyclic shifts of each other.
- This is solved by using Gold codes or Gold sequences (such as used in a GPS system).

Table of m-sequences

- Below we give a table of m-sequences. The table lists the feedback connection for a Fibonacci style connection. As an example the entry for a 5 stage shift register of [3, 5] means that the 3rd and 5th stages are combined to enter the first stage.



- This can also be written as a binary vector, namely 100101 where the positions containing a 1 indicate a connection. The first bit is always a '1' indicating that the first stage has the feedback. The last bit is also always a '1'. Sometimes this is converted to octal ($100101 = [45]_8$).

Table of m-sequences

The following feedback connections generate sequences of maximal length. The reciprocal of a shift register also produces a maximum-length sequence.

Sequence Length	Shift Register Size	Feedback	Octal
3	2	$x_n = x_{n-1} + x_{n-2}$	(111) 7
7	3	$x_n = x_{n-2} + x_{n-3}$	(1011) 13
7	3	$x_n = x_{n-1} + x_{n-3}$	(1101) 15
15	4	$x_n = x_{n-3} + x_{n-4}$	(10011) 23
15	4	$x_n = x_{n-1} + x_{n-4}$	(11001) 31
31	5	$x_n = x_{n-3} + x_{n-5}$	(100101) 45
31	5	$x_n = x_{n-2} + x_{n-5}$	(101001) 51
31	5	$x_n = x_{n-1} + x_{n-2} + x_{n-3} + x_{n-5}$	(111101) 75
31	5	$x_n = x_{n-2} + x_{n-3} + x_{n-4} + x_{n-5}$	(101111) 57
31	5	$x_n = x_{n-1} + x_{n-3} + x_{n-4} + x_{n-5}$	(110111) 67
31	5	$x_n = x_{n-1} + x_{n-2} + x_{n-4} + x_{n-5}$	(111011) 73

http://in.ncu.edu.tw/ncume_ee/digilogi/prbs.htm

Table of m-sequences

Stages	Connections (reverses omitted) (Octal representation in parenthesis)
3	[2, 3] (13)
4	[4, 3] (23)
5	[3, 5] (45), [2, 3, 4, 5] (57), [1, 3, 4, 5] (67)
6	[5, 6] (103), [1, 4, 5, 6] (147), [2, 3, 5, 6] (133)
7	[6, 7] (203), [4, 7] (211), [4, 5, 6, 7] (217), [2, 5, 6, 7] (247), [2, 4, 6, 7] (253) [1, 4, 6, 7] (313), [3, 4, 5, 7] (235), [2, 3, 4, 5, 6, 7] (277) , [1, 2, 4, 5, 6, 7] (357)
8	[8, 7, 6, 1], [8, 7, 5, 3], [8, 7, 3, 2], [8, 6, 5, 4], [8, 6, 5, 3], [8, 6, 5, 2] [8, 7, 6, 5, 4, 2], [8, 7, 6, 5, 2, 1]
9	[9, 5], [9, 8, 7, 2], [9, 8, 6, 5], [9, 8, 5, 4], [9, 8, 5, 1], [9, 8, 4, 2], [9, 7, 6, 4] [9, 7, 5, 2], [9, 6, 5, 3], [9, 8, 7, 6, 5, 3], [9, 8, 7, 6, 5, 1], [9, 8, 7, 6, 4, 3] [9, 8, 7, 6, 4, 2], [9, 8, 7, 6, 3, 2], [9, 8, 7, 6, 3, 1], [9, 8, 7, 6, 2, 1], [9, 8, 7, 5, 4, 3] [9, 8, 7, 5, 4, 2], [9, 8, 6, 5, 4, 1], [9, 8, 6, 5, 3, 2], [9, 8, 6, 5, 3, 1] [9, 7, 6, 5, 4, 3], [9, 7, 6, 5, 4, 2], [9, 8, 7, 6, 5, 4, 3, 1]
10	[10, 7], [10, 9, 8, 5], [10, 9, 7, 6], [10, 9, 7, 3], [10, 9, 6, 1], [10, 9, 5, 2], [10, 9, 4, 2] [10, 8, 7, 5], [10, 8, 7, 2], [10, 8, 5, 4], [10, 8, 4, 3], [10, 9, 8, 7, 5, 4], [10, 9, 8, 7, 4, 1] [10, 9, 8, 7, 3, 2], [10, 9, 8, 6, 5, 1], [10, 9, 8, 6, 4, 3], [10, 9, 8, 6, 4, 2] [10, 9, 8, 6, 3, 2], [10, 9, 8, 6, 2, 1], [10, 9, 8, 5, 4, 3], [10, 9, 8, 4, 3, 2] [10, 9, 7, 6, 4, 1], [10, 9, 7, 5, 4, 2], [10, 9, 6, 5, 4, 3], [10, 8, 7, 6, 5, 2] [10, 9, 8, 7, 6, 5, 4, 3], [10, 9, 8, 7, 6, 5, 4, 1], [10, 9, 8, 7, 6, 4, 3, 1] [10, 9, 8, 6, 5, 4, 3, 2], [10, 9, 7, 6, 5, 4, 3, 2]

http://in.ncu.edu.tw/ncume_ee/digilogi/prbs.htm

Zadoff-Chu Sequences

- Consider the sequence

$$x_n = e^{jM\pi n^2/N},\ n = 0, 1, ..., N-1, ...$$

where M is an integer relatively prime to N and N is even.

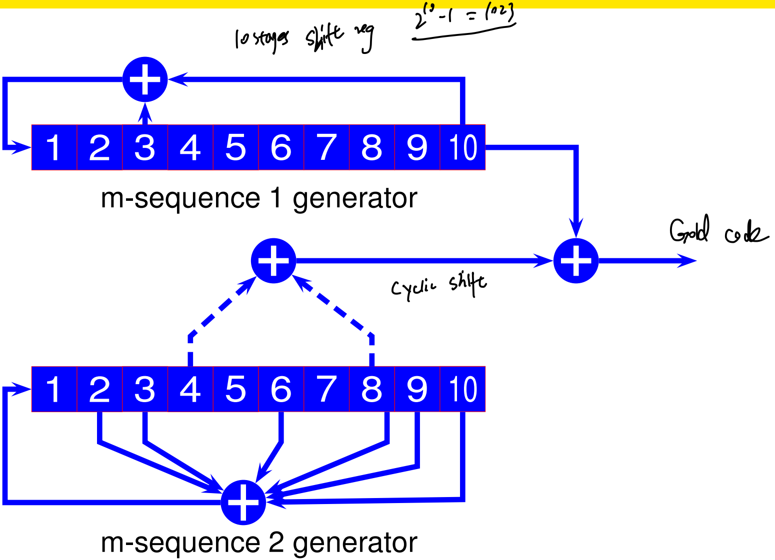
- Note that for *only if* N is even is $x_n = x_{n+N}$.
- As an example, suppose that $N = 8$ and $M = 3$ then the sequence is

$$\begin{aligned}\{x_n, n = 0, 1, \ldots, 7\} &= \left\{e^{j0\pi},\ e^{j3\pi/8},\ e^{j3\pi 4/8},\ e^{j3\pi 9/8}, e^{j3\pi 16/8}, e^{j3\pi 25/8}, e^{j3\pi 36/8}, e^{j3\pi 49/8}\right\} \\ &= \left\{e^{j\pi 0/8}, e^{j3\pi/8}, e^{j12\pi/8}, e^{j11\pi/8}, e^{j0\pi/8}, e^{j11\pi/8}, e^{j12\pi/8}, e^{j3\pi/8}\right\}\end{aligned}$$

Gold Codes

- Invented by Robert Gold
- Combines certain m-sequences together (mod 2)
- Many more sequences than m-sequences

Gold Codes used in GPS



Gold Codes used in GPS

- There are 1025 different Gold codes of length 1023
- These include the two m-sequences themselves and then 1023 the combination of the two with 1023 different shifts of one with respect to the other.

Each Satellite uses a particular Gold code (there are less than 36 Satellites)

Zadoff-Chu Sequences

uses in LTE $x_n = e^{j M \pi n^2 / N}$

- Consider the *periodic* autocorrelation of this sequence.
- The autocorrelation when the sequence is complex is

$$\begin{aligned} \theta_x(m) &= \sum_{k=0}^{N-1} x_k^* x_{k+m} \\ &= \sum_{k=0}^{N-1} x_k x_{k-m}^* \end{aligned}$$

where the indices are interpreted modulo N. That is, $x_N = x_0, \; x_{N+1} = x_1, \ldots$

Zadoff-Chu Sequences

- Then the periodic autocorrelation function is

$$\begin{aligned}
\theta_x(m) = \sum_{k=0}^{N-1} x_k^* x_{k+m} &= \sum_{k=0}^{N-1} \underbrace{e^{-jM\pi k^2/N}}_{x_k^*} \underbrace{e^{jM\pi(k+m)^2/N}}_{x_{k+m}} \\
&= \sum_{k=0}^{N-1} e^{jM\pi(-k^2+\underbrace{(k+m)^2}_{k^2+2mk+m^2})/N} \\
&= \sum_{k=0}^{N-1} e^{jM\pi(2mk+m^2)/N} \\
&= e^{jM\pi m^2/N} \sum_{k=0}^{N-1} e^{jM2\pi mk/N} \\
&= e^{jM\pi m^2/N} \sum_{k=0}^{N-1} [e^{jM2\pi m/N}]^k .
\end{aligned}$$

if m, N relating prime

m = lN

Assuming that $a \neq 1$ we have

$$\sum_{k=0}^{N-1} a^k = \begin{cases} \frac{a^N-1}{a-1}, & a \neq 1 \\ N, & a = 1. \end{cases}$$

If $Mm \neq N$ for any m, i.e. M is relatively prime to N, then $Mm/N \neq 1$ for any m then $e^{-jM2\pi m/N} \neq 1$.

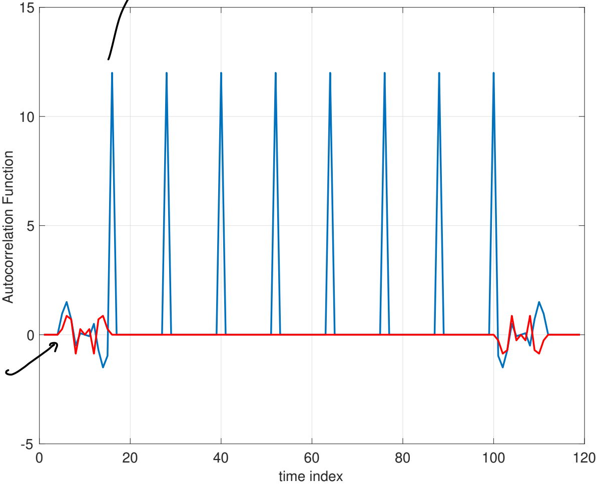
So

$$\begin{aligned}
\theta_x(m) &= e^{jM\pi m^2/N} \sum_{k=0}^{N-1} [e^{jM2\pi m/N}]^k. \\
&= e^{jM\pi m^2/N} \left[\frac{e^{jM2\pi m} - 1}{e^{jM2\pi m/N} - 1} \right]. \\
&= \begin{cases} 0, & m \neq 0, N, 2N, \ldots \\ N, & m = 0, N, 2N, \ldots \end{cases}
\end{aligned}$$

$e^{i\theta} = \cos\theta + i\sin\theta$

Correlation Function for $N = 12$

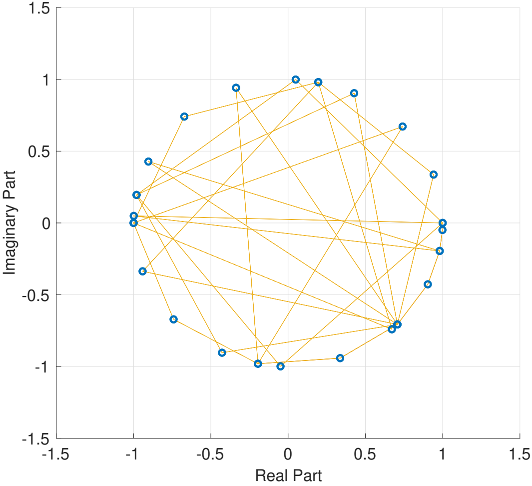
real part



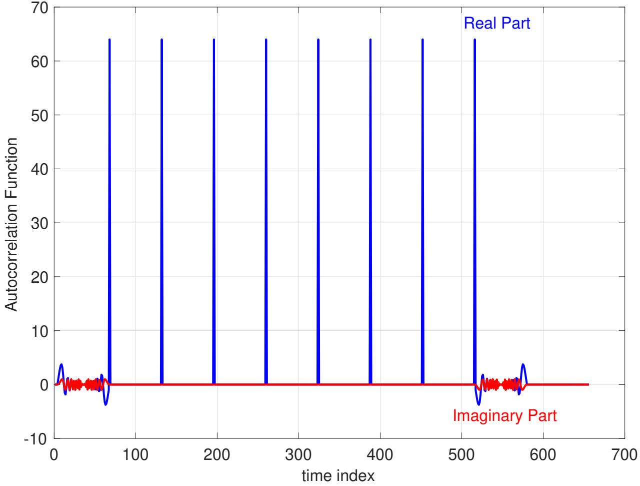
imaging part

Sequence for $N = 64$

HW



Correlation Function for $N = 64$



- The autocorrelation property is ideal but it requires the sequences to be complex with phases that are multiples of $1/N$.
- When N is odd the Zadoff-Chu sequences are defined as

$$x_n = e^{jM\pi n(n+1)/N}, \; n = 0, 1, ..., N-1, ...$$

- Again, only if N is odd does this sequence repeat. These sequences for N odd have the same autocorrelation as the N even case.
- Note that the phase of the sequences (even or odd lengths) is increasing quadratically with the index. This means that the frequency is linearly increasing.

Summary of Spreading Codes

Codes/Sequences	Property 1	Property 2	Property 3
m-sequences	Binary	Two-valued Periodic Autocorrelation (N, -1)	Relatively Small Number of Sequences
Gold Codes	Binary	Four Valued Periodic Autocorrelation	Large Number of Sequences ($N+2$).
Zadof Chu Codes	Nonbinary	Ideal Autocorrelation (N and 0)	Any Length

There are many other codes or sequences with useful properties. This include: Golay sequences, almost perfect autocorrelation sequences (APAS), Barker sequences, Kasami sequences.

Summary of Spreading Codes

Codes/Sequences	Property 1	Property 2	Property 3
m-sequences	Binary	Two-valued Periodic Autocorrelation (N, -1)	Relatively Small Number of Sequences
Gold Codes	Binary	Four Valued Periodic Autocorrelation	Large Number of Sequences ($N+2$).
Zadof Chu Codes	Nonbinary	Ideal Autocorrelation (N and 0)	Any Length

There are many other codes or sequences with useful properties. This include: Golay sequences, almost perfect autocorrelation sequences (APAS), Barker sequences, Kasami sequences.