

# A SIMPLE SCHEME TO EVALUATE PERIODIC CORRELATION VALUES FOR $m$ -SEQUENCES IN GF( $p$ )

Alois M.J. Goiser  
Johannes Philipp

TU-Vienna  
Institut für Allgemeine Elektrotechnik und Elektronik  
Abteilung für Angewandte Elektronik  
E-mail: agoiser@ps1.iaee.tuwien.ac.at.

## ABSTRACT

The presented scheme evaluates the periodic autocorrelation function for  $p$ -ary  $m$ -sequences and differ to the known schemes with respect to its simplicity and low computation afford. The approach to the presented scheme is from a heuristic nature. As examples the periodic autocorrelation function for ternary and quinary  $m$ -sequences are calculated.

## INTRODUCTION

In the introduction we briefly review [1], [2], [3], [5] the properties of  $p$ -ary  $m$ -sequences, with  $p$  a prime number and focus on the evaluation of the periodic autocorrelation function in the next section.

### A. Length of a $p$ -ary $m$ -Sequence

The sequence-elements of an  $p$ -ary  $m$ -sequence are the elements of the galois-field GF( $p$ ). The maximum achievable sequence-length or period is  $L_p = p^r - 1$ . Generating a sequence of this length with a shift register generator means that the generator subsequently passes all possible states except the all zero state.

$$L_p = p^r - 1 \quad (1)$$

### B. Balance Property of the $p$ -ary $m$ -sequence

The occurrence of the zero-element in an  $p$ -ary  $m$ -sequence is  $S_0 = p^{r-1} - 1 = \frac{1}{p}(L_p + 1) - 1$ , and the other elements appear with  $S_1 = p^{r-1} = \frac{1}{p}(L_p + 1)$ . It is noticeable that the zero-element appear once less than the other elements.

### C. Cyclic Shift of $p$ -ary $m$ -Sequences

According to binary  $m$ -sequences, there are  $L_p = p^r - 1$  cyclic shifts possible with  $p$ -ary  $m$ -sequences.

### D. Shift and Add Property of $p$ -ary $m$ -Sequences

The shift- and add property of a binary  $m$ -sequence translates to a shift- and subtract property for a  $p$ -ary  $m$ -sequence.

### E. Runbalance of a $p$ -ary $m$ -Sequence

The runbalance property is not simply convertible to  $p$ -ary  $m$ -sequences, because  $p$ -ary  $m$ -sequences break into  $p - 1$  sub-sequences of equal length.

### F. Periodic Autocorrelation Function of $p$ -ary $m$ -Sequences

The properties of the periodic autocorrelation function (PACF) of binary  $m$ -sequences are not directly mapable to  $p$ -ary  $m$ -sequences because of the well known decomposition [5] of  $p$ -ary  $m$ -sequences into  $p - 1$  sub-sequences of length:

$$L_{pu} = \frac{L_p}{p-1} = \frac{p^r - 1}{p-1} \quad (2)$$

The decomposition into sub-sequences has a major influence on the PACF, and makes the derivative of the PACF more complex.

## EVALUATION OF THE PERIODIC AUTOCORRELATION FUNCTION OF $P$ -ARY $M$ -SEQUENCES

### G. Unipolar Sequences

To verify the derivative of the PACF the ternary and quinary  $m$ -sequences in example 1.1 and 1.2 are used.

**EXAMPLE 1.1 (TERNARY  $m$ -SEQUENCE)** The ternary  $m$ -sequence [3] is derived from the primitive polynomial  $f(x) = x^3 + 2x + 1$ . The length of the sequence is  $L_p = 26$ . ( $L_p = 26, p = 3, r = 3$ .)

$$a(n) = [1\ 1\ 1\ 0\ 2\ 1\ 1\ 2\ 1\ 0\ 1\ 0\ 0\ | \\ 2\ 2\ 2\ 0\ 1\ 2\ 2\ 1\ 2\ 0\ 2\ 0\ 0] \quad (3)$$

The length of the sub-sequences in (3) are derived with (2) to  $L_{pu} = 13$ .

**EXAMPLE 1.2 (QUINARY  $m$ -SEQUENCE)** The quinary  $m$ -sequence [3] is derived from the primitive polynomial  $f(x) = x^2 + x + 2$ . The length of the sequence is  $L_p = 24$ . ( $L_p = 24, p = 5, r = 2$ .)

$$a(n) = [1\ 2\ 1\ 1\ 4\ 0 \mid 3\ 1\ 3\ 3\ 2\ 0 \mid 4\ 3\ 4\ 4\ 1\ 0 \mid 2\ 4\ 2\ 2\ 3\ 0] \quad (4)$$

The length of the sub-sequences in (4) are derived with (2) to  $L_{pu} = 6$ .

The examples show, that in the periode  $L_p$  of the  $p$ -ary  $m$ -sequence ordered pairs of  $[\tilde{a}(n), \tilde{a}(n+k)]$  for  $0 \leq n \leq L_p$  occur, with frequencies depicted in Tab.1. The frequencies of the ordered pairs are termed *pair-frequencies*.

**DEFINITION 1.1 (LINEAR DEPENDENCY)** Equation (5) indicates the linear dependence as it shows that the sub-sequences are related in the following way: The primitive element is taken to the power of  $t$  and multiplied (mod  $p$ ) with each element of the finite field. The zero-element maps always to the zero-element.

$$\tilde{a}(n+k) = \mu^t \cdot a(n) \quad (5)$$

$\mathbf{k \not\equiv 0 \pmod{L_{pu}}}$ The occurrence of the pair $[0, 0]$ in the sequence is $(p^{r-2} - 1)$ . All other pairs occur with frequency $p^{r-2}$ .
$\mathbf{k \equiv 0 \pmod{L_{pu}}, k \not\equiv 0 \pmod{L_p}$ Applying (5) with $\mu$ a primitive element of $\mathbf{GF}(p)$ and $t$ , dependent on the chosen sub-sequence is a natural number in the range of $1 \leq t \leq p - 2$ . In this case the occurrence of the pair $[0, 0]$ is exactly $(p^{r-1} - 1)$ and all other pairs $[a(n), \mu^t \cdot a(n)]$ of non-vanishing elements appear with frequency $p^{r-1}$ .

Table 1. Pair-Frequencies  $[a(n), \mu^t \cdot a(n)]$  in a  $p$ -ary  $m$ -Sequence.

**EXAMPLE 1.3 (LINEAR DEPENDENCE)** The derivative of the linear dependence of the sub-sequences in example 1.1 are depicted in (6) and (7). The smallest primitive element  $\mu$  in  $\mathbf{GF}(3)$  is the element 2.

$$L_{pu} = 13, p = 3, t \in \{1, \dots, p-2\} \rightarrow t = 1$$

$$1 \cdot \mu^1 = 1 \cdot 2 = 2 \quad (1 \mapsto 2) \quad (6)$$

$$2 \cdot \mu^1 = 2 \cdot 2 = 4 \equiv 1 \pmod{3} \quad (2 \mapsto 1) \quad (7)$$

Example 1.3 shows, that each ternary  $m$ -sequence breaks up into two linear dependent sub-sequences of length 13. The linear dependence is given with the following mapping:

$$\begin{pmatrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \end{pmatrix}_{t=1}^{\mu=2} \quad (8)$$

**EXAMPLE 1.4 (LINEAR DEPENDENCE)** The linear dependence of the sub-sequences in example 1.2 are derived with the smallest primitive element  $\mu = 2$  in  $\mathbf{GF}(5)$ .

$$L_{pu} = 6, p = 5, t \in \{1, \dots, p-2\} \rightarrow t = 1, 2, 3.$$

$t = 1$	
Derivative	Mapping
$1 \cdot \mu^1 \equiv 2 \pmod{5}$	$(1 \mapsto 2)$
$2 \cdot \mu^1 \equiv 4 \pmod{5}$	$(2 \mapsto 4)$
$3 \cdot \mu^1 \equiv 1 \pmod{5}$	$(3 \mapsto 1)$
$4 \cdot \mu^1 \equiv 3 \pmod{5}$	$(4 \mapsto 3)$
$t = 2$	
Derivative	Mapping
$1 \cdot \mu^2 \equiv 4 \pmod{5}$	$(1 \mapsto 4)$
$2 \cdot \mu^2 \equiv 3 \pmod{5}$	$(2 \mapsto 3)$
$3 \cdot \mu^2 \equiv 2 \pmod{5}$	$(3 \mapsto 2)$
$4 \cdot \mu^2 \equiv 1 \pmod{5}$	$(4 \mapsto 1)$
$t = 3$	
Derivative	Mapping
$1 \cdot \mu^3 \equiv 3 \pmod{5}$	$(1 \mapsto 3)$
$2 \cdot \mu^3 \equiv 1 \pmod{5}$	$(2 \mapsto 1)$
$3 \cdot \mu^3 \equiv 4 \pmod{5}$	$(3 \mapsto 4)$
$4 \cdot \mu^3 \equiv 2 \pmod{5}$	$(4 \mapsto 2)$

Table 2. Linear dependence of the sub-sequences of the quinary  $m$ -Sequence in example 1.2.

Example 1.4 shows that each quinary  $m$ -sequence break into four linear dependent sub-sequences with periode  $L_{pu} = 6$ . The linear dependence of the sub-sequences are listed in (9).

$$\begin{pmatrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 3 \end{pmatrix}_{t=1}^{\mu=2} \begin{pmatrix} 1 & \mapsto & 4 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \\ 4 & \mapsto & 1 \end{pmatrix}_{t=2}^{\mu=2} \begin{pmatrix} 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 4 \\ 4 & \mapsto & 2 \end{pmatrix}_{t=3}^{\mu=2} \quad (9)$$

Each mapping is related with the help of parameter  $t$  to his own sub-sequence. The condition (5) defined in Def.1.1 holds also for  $k = l \cdot L_{pu}$  with  $l \in \{1, \dots, p-1\}$ . Owing to this we get Tab.3 for the chosen quinary  $m$ -sequence.

Tab.3 shows that the second sub-sequence is linear dependent to the first sub-sequence with  $t = 3$  and the third sub-sequence is linear dependent to the first sub-sequence with  $t = 2$  and the fourth sub-sequence is linear dependent to the first sub-sequence with  $t = 1$ .

In general the mapping, maps each element  $\alpha_i$  of a cyclic group  $\mathbf{GF}^*(p)$  as an individual of an arbitrary galois-field  $\mathbf{GF}(p)$  injective on an element of the same group (isomorph mapping).

With the help of this heuristic mapping approach we define a *mapping product* in Def.1.2.

$n = 1, k = L_{pu}$
$\bar{a}(n+k) = \mu^t \cdot a(n)$
$a(1+6) = \mu^t \cdot a(1)$
$3 = \mu^t \cdot 1 \rightarrow t = 3$
$n = 1, k = 2 \cdot L_{pu}$
$\bar{a}(n+k) = \mu^t \cdot a(n)$
$a(1+2 \cdot 6) = \mu^t \cdot a(1)$
$4 = \mu^t \cdot 1 \rightarrow t = 2$
$n = 1, k = 3 \cdot L_{pu}$
$\bar{a}(n+k) = \mu^t \cdot a(n)$
$a(1+3 \cdot 6) = \mu^t \cdot a(1)$
$2 = \mu^t \cdot 1 \rightarrow t = 1$

Table 3. Linear Dependency for the sub-sequences of the chosen  $m$ -sequence in example 1.2.

**DEFINITION 1.2 (MAPPING PRODUCT)** *The two columns of the mapping are treated as vectors. With these two vectors a mapping product  $\Gamma(\mu, t)$  can be defined in the sense of the inner product of two vectors.*

$\alpha_i \mapsto \alpha_j$  with:  $i = j \in \{1, \dots, p-1\}; \alpha_i, \alpha_j \in \mathbf{GF}^r(p)$

$$\Gamma(\mu, t) = \alpha_i \cdot \alpha_j$$

When we divide the mapping product by  $p-1$ , we refer to this as normalized mapping product.

$$\Gamma(\mu, t, p) = \frac{1}{p-1} \cdot \Gamma(\mu, t)$$

**EXAMPLE 1.5 (MAPPING PRODUCT FOR EXAMPLE 1.1)**

$$\begin{aligned} \Gamma(\mu, t) &: \Gamma(2, 1) = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 4 \\ \Gamma(\mu, t, p) &: \Gamma(2, 1, 3) = 2 \end{aligned} \quad (10)$$

**EXAMPLE 1.6 (MAPPING PRODUCT FOR EXAMPLE 1.2)**

$$\begin{aligned} \Gamma(2, 1, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 4 \\ 1 \\ 3 \end{pmatrix} = \frac{25}{4} \\ \Gamma(2, 2, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 3 \\ 2 \\ 1 \end{pmatrix} = \frac{20}{4} \\ \Gamma(2, 3, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \\ 4 \\ 2 \end{pmatrix} = \frac{25}{4} \end{aligned} \quad (11)$$

Due to the linear dependence of the sub-sequence the PACF of  $p$ -ary  $m$ -sequences have a constant value  $\check{\phi}_{aa}(i)$ , if the time-shift  $k$  is not a multiple of the length of the

sub-sequence  $L_{pu}$ . If the time-shift  $k$  is a multiple of the length of the sub-sequence  $L_{pu}$ , then  $p-1$  other correlation values  $\check{\phi}_{aa}(2), \check{\phi}_{aa}(3), \dots$  occur, but not necessarily different.

The calculation of the PACF is based on the normalized mapping products and is verified for the ternary and quinary  $m$ -sequence in example 1.1 and 1.2. For the calculation of the PACF we have assigned amplitudes  $a_i \in \{a_0, a_1, \dots, a_{p-1}\}$  to the elements  $\alpha_i \in \mathbf{GF}(p)$ . We assume *unipolar*  $p$ -ary  $m$ -sequences and assign the elements of  $\mathbf{GF}(p)$  the amplitude of their own value.

The peak of the correlation function  $\hat{\phi}_{aa}$  (main-value corresponds to time-shift  $k = 0$ ) follows with the *pair-frequency* listed in Tab.1:

$$\hat{\phi}_{aa} = p^{r-1} \cdot \sum_{i=0}^{p-1} a_i^2 - a_0^2 \quad (12)$$

The constant autocorrelation side-value  $\check{\phi}_{aa}(1)$  (corresponds to a time-shift  $k \neq 0$ ) for time-shifts  $k$  that are not multiples of the length of the sub-sequence  $L_{pu}$  is:

$$\begin{aligned} \check{\phi}_{aa}(1) &= \phi_{aa}(k \not\equiv 0 \pmod{L_{pu}}) = \\ &= p^{r-2} \cdot \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} a_i a_j - a_0^2 \end{aligned} \quad (13)$$

For all other side-values  $\check{\phi}_{aa}(i)$  with the assumption that the time-shifts are multiples of the sub-sequence length  $L_{pu}$  follows:

$$\begin{aligned} \check{\phi}_{aa}(i) &= \phi_{aa}(k \equiv 0 \pmod{L_{pu}}) = \\ &= \Gamma(\mu, t, p) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) \end{aligned} \quad (14)$$

The right term in the product in (14) corresponds to the non-zero occurrence frequencies of the elements from  $\mathbf{GF}(p)$  in the sequence. Corresponding to the balance-property, there are  $p^{r-1}-1$  zeros in the whole length  $(p^r-1)$  of the sequence. This amount of zeros has to be subtracted to achieve the product term on the right side.

The normalized mapping-product  $\Gamma(\mu, t, p)$  can be treated as average correlation portion per sequence-element (accept the zero-element) in the PACF.

The parameter  $t$  in the mapping-product points to the index of the correlation side-value with  $i = t+1$  for  $1 \leq t \leq p-2$ .

To verify the calculation scheme we calculate the PACF for the ternary and quinary  $m$ -sequences.

EXAMPLE 1.7 (PACF FOR EXAMPLE 1.1)

$$\begin{aligned}
 \hat{\phi}_{aa} &= p^{r-1} \cdot \sum_{i=0}^{p-1} a_i^2 - a_0^2 \quad \text{if: } a_0 = 0 \\
 &= 3^2 \cdot \sum_{i=1}^{p-1} a_i^2 = 9 \cdot (1 + 4) = 45 \\
 \check{\phi}_{aa}(1) &= p^{r-2} \cdot \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} a_i a_j - a_0^2 \quad \text{if: } a_0 = 0 \\
 &= 3^1 \cdot \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} a_i a_j = \\
 &= 3 \cdot (1 + 2 + 2 + 4) = 27 \\
 \check{\phi}_{aa}(2) &= \Gamma(\mu, t, p) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= \Gamma(2, 1, 3) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= 2 \cdot 3^3 \cdot \left(1 - \frac{1}{3}\right) = 36
 \end{aligned}$$

Summarized:

$$\phi_{aa}(k) = \begin{cases} \hat{\phi}_{aa} & = 45 \quad \dots k \equiv 0 \pmod{L_p} \\ \check{\phi}_{aa}(1) & = 27 \quad \dots k \not\equiv 0 \pmod{L_p, L_{pu}} \\ \check{\phi}_{aa}(2) & = 36 \quad \dots k \equiv 0 \pmod{L_{pu}} \end{cases}$$

EXAMPLE 1.8 (PACF FOR EXAMPLE 1.2)

$$\begin{aligned}
 \hat{\phi}_{aa} &= p^{r-1} \cdot \sum_{i=0}^{p-1} a_i^2 - a_0^2 \quad \text{if: } a_0 = 0 \\
 &= 5^1 \cdot \sum_{i=1}^{p-1} a_i^2 = 5 \cdot (1 + 4 + 9 + 16) = 150 \\
 \check{\phi}_{aa}(1) &= p^{r-2} \cdot \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} a_i a_j - a_0^2 \quad \text{if: } a_0 = 0 \\
 &= 5^0 \cdot \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} a_i a_j = \\
 &= 1 \cdot (10 + 20 + 30 + 40) = 100 \\
 \check{\phi}_{aa}(2) &= \Gamma(\mu, t, p) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= \Gamma(2, 1, 5) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= \frac{25}{4} \cdot 5^2 \cdot \left(1 - \frac{1}{5}\right) = 125 \\
 \check{\phi}_{aa}(3) &= \Gamma(2, 2, 5) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= \frac{20}{4} \cdot 5^2 \cdot \left(1 - \frac{1}{5}\right) = 100 = \check{\phi}_{aa}(1) \\
 \check{\phi}_{aa}(4) &= \Gamma(2, 3, 5) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\
 &= \frac{25}{4} \cdot 5^2 \cdot \left(1 - \frac{1}{5}\right) = 125 = \check{\phi}_{aa}(2)
 \end{aligned}$$

Summarized:

$$\phi_{aa}(k) = \begin{cases} \hat{\phi}_{aa} & = 150 \quad \dots k \equiv 0 \pmod{L_p} \\ \check{\phi}_{aa}(1) & = 100 \quad \dots \begin{matrix} k \not\equiv 0 \pmod{L_p, L_{pu}} \\ k \equiv 0 \pmod{2L_{pu}} \end{matrix} \\ \check{\phi}_{aa}(2) & = 125 \quad \dots k \equiv 0 \pmod{L_{pu}, 3L_{pu}} \end{cases}$$

The general shape of the PACF for unipolar  $p$ -ary  $m$ -sequences is depicted in Fig.1. If we set  $\check{\phi}_{ss}(3) = \check{\phi}_{ss}(1)$  and change the sequence index  $ss$  to  $aa$  than Fig.1 visualizes the results for example 1.8.

H. Bipolar Sequences

To remove the mean value of unipolar  $p$ -ary  $m$ -sequences we have to assign each element  $\alpha_i \in \mathbf{GF}(p)$  ( $p > 2$ ) its amplitude symmetric value with respect to zero. The transform in (15) changes a unipolar  $p$ -ary  $m$ -sequence to a bipolar  $p$ -ary  $m$ -sequence.

$$a_i = \begin{cases} \alpha_i & \text{if: } \alpha_i \leq \frac{p-1}{2} \\ \alpha_i - p & \text{else} \end{cases} \quad p > 2 \quad (15)$$

This transform changes the equation for the  $\hat{\phi}_{aa}$  and  $\check{\phi}_{aa}(1)$  while the products  $a_i a_j$  compensate each other:

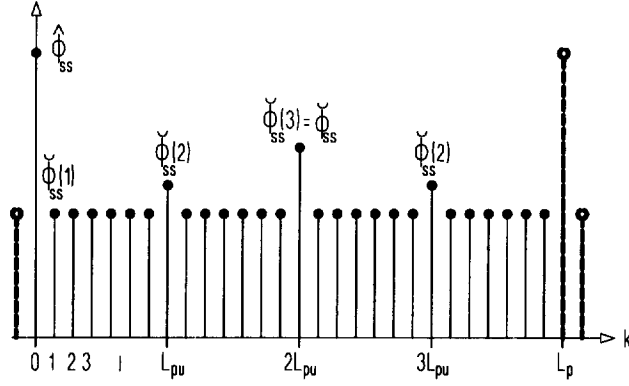


Figure 1. General Shape of the PACF of a  $p$ -ary  $m$ -sequence  $s(n)$ .

$$\begin{aligned}\hat{\phi}_{aa} &= p^{r-1} \cdot \sum_{i=0}^{p-1} a_i^2 - a_0^2 = p^r \cdot \frac{p^2 - 1}{12} \\ \check{\phi}_{aa}(1) &= \phi_{aa}(k \not\equiv 0 \pmod{L_{pu}}) = \\ &= p^{r-2} \cdot \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} a_i a_j - a_0^2 = 0\end{aligned}\quad (16)$$

In the calculation for  $\check{\phi}_{aa}(i)$  we have simply to change the normalized mapping-product  $\Gamma(\mu, t, p)$  to the normalized and symmetric mapping-product  $\Gamma_s(\mu, t, p)$ .

$$\begin{aligned}\check{\phi}_{aa}(i) &= \phi_{aa}(k \equiv 0 \pmod{L_{pu}}) = \\ &= \Gamma_s(\mu, t, p) \cdot p^r \cdot \left(1 - \frac{1}{p}\right)\end{aligned}\quad (17)$$

EXAMPLE 1.9 (PACF FOR EXAMPLE 1.1) *The transformation*

$$0 \mapsto 0, 1 \mapsto 1, 2 \mapsto -1 \quad (18)$$

changes the sequence to a symmetric ternary  $m$ -sequence.

$$\begin{aligned}a_s(n) &= [1110 - 111 - 110100 - 1 - 1 - 10 \\ &\quad 1 - 1 - 11 - 10 - 100]\end{aligned}\quad (19)$$

The main-value of the correlation function  $\hat{\phi}_{aa}$  is:

$$\hat{\phi}_{aa} = \phi_{aa}(0) = p^r \frac{p^2 - 1}{12} = 3^3 \cdot \frac{3^2 - 1}{12} = 18 \quad (20)$$

The constant side-value  $\check{\phi}_{aa}(1)$  vanishes due to the zero mean property of the sequence. To calculate the constant side-value  $\check{\phi}_{aa}(2)$  we need the normalized and symmetric mapping-product  $\Gamma_s(\mu, t, p)$ . With the help of  $\Gamma(\mu, t, p)$  we can easily derive  $\Gamma_s(\mu, t, p)$ ,

$$\begin{aligned}\Gamma(2, 1, 3) &= \frac{1}{2} \cdot \binom{1}{2} \cdot \binom{2}{1} \\ \mapsto \Gamma_s(2, 1, 3) &= \frac{1}{2} \cdot \binom{1}{-1} \cdot \binom{-1}{1} = -1\end{aligned}\quad (21)$$

and  $\check{\phi}_{aa}(2)$  follows:

$$\begin{aligned}\check{\phi}_{aa}(2) &= \phi_{aa}(k \equiv 0 \pmod{L_{pu}}) = \\ &= \Gamma_s(2, 1, 3) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\ &= -1 \cdot 3^3 \cdot \left(1 - \frac{1}{3}\right) = -18 = -\hat{\phi}_{aa}\end{aligned}\quad (22)$$

The  $\check{\phi}_{aa}(2)$  equals the negative  $\hat{\phi}_{aa}$  for a time-shift  $k \equiv 0 \pmod{L_{pu}}$ .

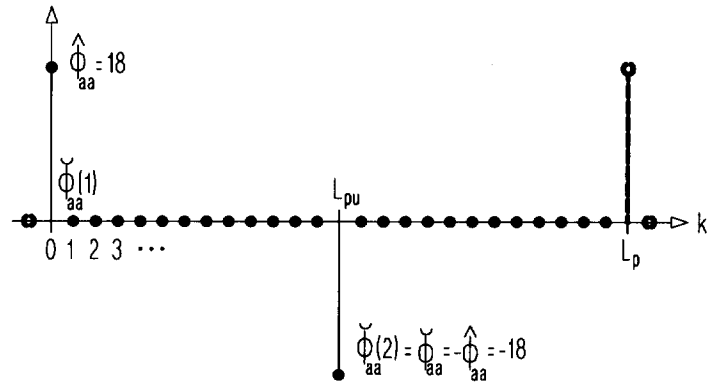


Figure 2. PACF for the ternary, symmetric  $m$ -sequence corresponding to example 1.9.

The PACF for example 1.9 is shown in Fig.2 and represents the general shape of the PACF for all ternary and symmetric  $m$ -sequences.

From example 1.9 the generalization follows:

The general shape of the PACF for a symmetric ternary  $m$ -sequences is zero ( $\check{\phi}_{aa}(1) = 0$ ), except for the main-value (no time-shift) and at the time-shift  $L_{pu}$ , where the negative main-value occurs ( $\check{\phi}_{aa}(2) = -\hat{\phi}_{aa} = -2 \cdot 3^{r-1}$ ).

EXAMPLE 1.10 (PACF FOR EXAMPLE 1.2) *The transformation*

$$0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto -2, 4 \mapsto -1 \quad (23)$$

changes the sequence to a symmetric quinary  $m$ -sequence.

$$\begin{aligned}a_s(n) &= [1 2 1 1 -1 0 | -2 1 -2 -2 2 0 | \\ &\quad -1 -2 -1 -1 1 0 | 2 -1 2 2 -2 0]\end{aligned}\quad (24)$$

The main-value of the correlation function  $\hat{\phi}_{aa}$  is:

$$\hat{\phi}_{aa} = \phi_{aa}(0) = p^r \cdot \frac{p^2 - 1}{12} = 5^2 \cdot \frac{5^2 - 1}{12} = 50 \quad (25)$$

The constant side-value  $\check{\phi}_{aa}(1)$  vanishes due to the zero mean property of the sequence. To calculate the constant side-values  $\check{\phi}_{aa}(2)$ ,  $\check{\phi}_{aa}(3)$  and  $\check{\phi}_{aa}(4)$  we need the normalized and symmetric mapping-product  $\Gamma_s(\mu, t, p)$ . With the help of  $\Gamma(\mu, t, p)$  in (11) we can easily derive  $\Gamma_s(\mu, t, p)$ :

$$\begin{aligned} \Gamma_s(2, 1, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ -2 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 1 \\ -2 \end{pmatrix} = 0, \\ \Gamma_s(2, 2, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ -2 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} -1 \\ -2 \\ 2 \\ 1 \end{pmatrix} = -\frac{10}{4}, \quad (26) \\ \Gamma_s(2, 3, 5) &= \frac{1}{4} \cdot \begin{pmatrix} 1 \\ 2 \\ -2 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 1 \\ -1 \\ 2 \end{pmatrix} = 0 \end{aligned}$$

The normalized mapping-products show, that the  $\check{\phi}_{aa}(2)$  and  $\check{\phi}_{aa}(4)$  must be zero and only  $\check{\phi}_{aa}(3)$  at the time-shift  $k \equiv 0 \pmod{2L_{pu}}$  is not equal zero.

With  $\Gamma_s(2, 2, 5)$  in (26) we derive:

$$\begin{aligned} \check{\phi}_{aa}(3) &= \phi_{aa}(k \equiv 0 \pmod{2L_{pu}}) = \\ &= \Gamma_s(2, 2, 5) \cdot p^r \cdot \left(1 - \frac{1}{p}\right) = \\ &= -\frac{10}{4} \cdot 5^2 \cdot \left(1 - \frac{1}{5}\right) = -50 = -\hat{\phi}_{aa} \quad (27) \end{aligned}$$

The shape of the PACF of a symmetric quinary  $m$ -sequence is similar to the shape of the PACF of the symmetric ternary  $m$ -sequence and is sketched in Fig.3. This allows the generalization:

The general shape of the PACF for a symmetric quinary  $m$ -sequences is zero ( $\check{\phi}_{aa}(1) = 0$ ), except for the main-value (no time-shift) and at the time-shift  $2L_{pu}$ , where the negative main-value occurs ( $\check{\phi}_{aa}(3) = -\hat{\phi}_{aa} = -2 \cdot 5^r$ ).

### CONCLUSION

A simple scheme to evaluate the periodic autocorrelation functions for  $p$ -ary  $m$ -sequences was presented. This scheme is based on *mapping-products* defined in the paper. These mapping-products are simple to evaluate for uniform and symmetric  $p$ -ary  $m$ -sequences and indicate if

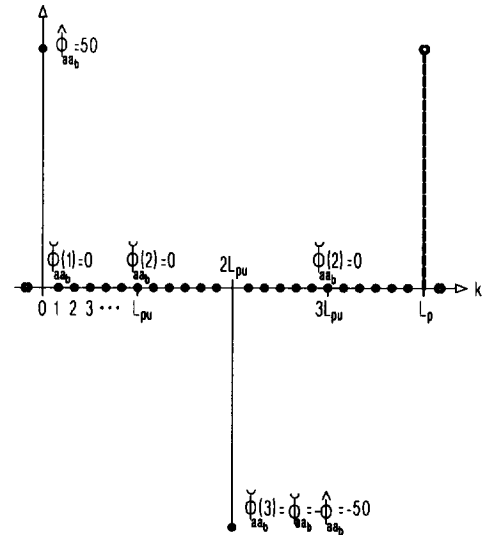


Figure 3. PACF of the quinary, symmetric  $m$ -sequence corresponding to example 1.2.

a correlation value for time-shifts unequal to zero and less the sequence length is not zero. This allows a quick decision if a correlation value has to be calculated and results in a fast computation algorithm.

### ACKNOWLEDGEMENT

The authors are thankful to Prof. Franz Seifert for his useful comments.

### GLOSSARY

$p$	...	prime number.
$r$	...	power of the polynomial.
$L_p$	...	length of the $p$ -ary $m$ -sequence.
$L_{pu}$	...	length of the sub-sequences of an $p$ -ary $m$ -sequence.
$a(n)$	...	$p$ -ary $m$ -sequence.
$\alpha$	...	element of $\mathbf{GF}(p)$ .
$\mu$	...	primitive element of $\mathbf{GF}(p)$ .
$a \equiv b \pmod{m}$	...	Congruence.
$a \not\equiv b \pmod{m}$	...	Not congruent.
$\Gamma(\mu, t, p)$	...	Mapping-product.
$\mathbf{GF}(p)$	...	Galois-field.
$\mathbf{GF}^*(p)$	...	Group of elements in Galois-field.
$\hat{\phi}_{aa}$	...	Main-correlation (time-shift zero).
$\check{\phi}_{aa}(i)$	...	Side-correlation.

### REFERENCES

- [1] S. Golomb, *Shift Register Sequences*, Holden Day Inc., (1967).
- [2] Rudolf Lidl, Harald Niederreiter, *Finite Fields*, Addison Wesley, (1983).
- [3] H.D.Lüke, *Korrelationssignale*, Springer Verlag, (1992).
- [4] J. Philipp, *Grundlagen der Spread-Spectrum Codefolgen*, Master-Thesis, IAEE-359/2, (1995).
- [5] F.J. Mac Williams, N.J.A. Sloane, *Pseudo-Random Sequences and Arrays*, Proceedings IEEE, Vol.64, 1715-1729, (1976).