

Partial Correlations of Galois Ring Sequences

UNESCO-CIMPA WORKSHOP ON
SEQUENCES
ANKARA, TURKEY

Serdar Boztaş

August 28, 2008

The plan

- Introduction.
- Periodic and Partial Periodic Correlations.
- The first and the second moments.
- Galois Rings
- Family A: Maximal length sequences over \mathbf{Z}_4 .
- Family B and C.
- Conclusions.

Periodic Correlation Function

We consider a q -ary family of M sequences of period N ,

$$\{ s_1, \dots, s_M \}, \quad s_i \in Z_q^N, \quad 1 \leq i \leq M$$

with $s_1 = (s_1(0), \dots, s_1(N-1))$, where Z_q is the ring of integers modulo q .

Periodic correlation function:

$$C_{i,j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t \oplus \tau) - s_j(t)}$$

where $\omega = \exp(2\pi j/4) = \sqrt{-1}$ is a primitive fourth root of unity and where \oplus denotes addition modulo N .

The Partial Correlation Function

Definition 1 *The periodic partial correlation function of s_i with s_j at shift τ and offset k with correlation length $L \leq N$ is given by*

$$P_{i,j}(\tau, k, L) = \sum_{t=k}^{k+L-1} \omega^{s_i(t \oplus \tau) - s_j(t)}, \quad 1 \leq i \leq j \leq M,$$

where \oplus denotes addition modulo N , and $0 \leq \tau \leq N - 1$.

The Partial Correlation and Its First Moment

Definition 2 *The first moment of the partial correlation function in Definition 1 is given by,*

$$\langle P_{i,j}(\tau, k, L) \rangle_k = \frac{1}{2^n - 1} \sum_{k=0}^{2^n - 2} P_{i,j}(\tau, k, L) \triangleq \overline{P_{i,j}(\tau, L)}$$

while its second absolute moment is given by

$$\langle |P_{i,j}(\tau, k, L)|^2 \rangle_k = \frac{1}{2^n - 1} \sum_{k=0}^{2^n - 2} |P_{i,j}(\tau, k, L)|^2$$

The notation $\langle f(k) \rangle_k$ denotes an average over all possible values of k of the argument f .

\mathbf{Z}_4 and its extension

- $GR(4, n)$ as opposed to $\mathbf{GF}(2^n)$.
- Trace functions.
- $\beta \in \mathbf{GR}(4, n)$ of order $2^n - 1$: $\alpha \in \mathbf{GF}(2^n)$ of order $2^n - 1$.
- m-sequence $tr(x) = tr(\alpha^i), 0 \leq i \leq 2^n - 1$,
- m-sequences over \mathbf{Z}_4 : $Tr(a\beta^i), 0 \leq i \leq 2^n - 1, a \in \mathbf{GR}(4, n)$.

\mathbf{Z}_4 m-sequences

Definition 3 *Let*

$$\gamma_i = \begin{cases} 1 + 2\beta^i, & 0 \leq i \leq 2^n - 2 \\ 1, & i = 2^n - 1 \\ 2, & i = 2^n \end{cases},$$

the \mathbf{Z}_4 maximal length sequence family is defined as

$$a_i(t) = \text{Tr}_1^n(\gamma_i \beta^t), \quad t = 0, 1, \dots, 2^n - 2. \quad (1)$$

Henceforth, we use:

\oplus : the addition operation in \mathbf{Z}_4 and

$+$: either the addition operation in \mathbf{Z}_2 or the ordinary addition operation in \mathbf{R} .

The First Moment for Family A

Theorem 1 *The first moment obeys*

$$\langle P_{i,j}(\tau, k, L) \rangle_k = \frac{L}{2^n - 1} C_{i,j}(\tau),$$

and therefore, for Family A, it simply takes on values proportional to the values in periodic correlation distribution with the same multiplicities. These multiplicities were given in a previous lecture.

Proof

We have

$$\begin{aligned}\overline{P_{i,j}(\tau, L)} &= \frac{1}{2^n - 1} \sum_{k=0}^{2^n - 2} P_{i,j}(\tau, k, L) \\ &= \frac{1}{2^n - 1} \sum_{k=0}^{2^n - 2} \sum_{t=0}^{L-1} \omega^{s_i(k \oplus t \oplus \tau) - s_j(k \oplus t)} \\ &= \frac{1}{2^n - 1} \sum_{t=0}^{L-1} \sum_{k=0}^{2^n - 2} \omega^{s_i(k \oplus t \oplus \tau) - s_j(k \oplus t)} \\ &= \frac{1}{2^n - 1} \sum_{t=0}^{L-1} C_{i,j}(\tau) = \frac{L}{2^n - 1} C_{i,j}(\tau).\end{aligned}$$

The Second Moment

For Binary m-sequences, we have a well known result:

Proposition 1 *For the binary m-sequence s_1 , we have*

$$\langle |P_{1,1}(\tau, k, L)|^2 \rangle_k = L \left(1 - \frac{L-1}{2^n-1} \right),$$

when $\tau \neq 0 \pmod{2^n-1}$.

It would be nice to have a similar result for Family A.

Proof of Binary m -sequence Result

We have

$$(2^n - 1) \langle |P(\tau, k, L)|^2 \rangle_k = \sum_{k=0}^{2^n - 2} |P(\tau, k, L)|^2$$

and

$$|P(\tau, k, L)|^2 = \sum_{t, t'=0}^{L-1} (-1)^{\text{tr}[(\alpha^\tau + 1)(\alpha^{t+k} + \alpha^{t'+k})]}$$

As k ranges over $[0, 2^n - 2]$ the pair $(t + k, t' + k)$ ranges over $[0, 2^n - 2] \times [0, 2^n - 2]$ L times. Therefore

$$\sum_{k=0}^{2^n - 2} |P(\tau, k, L)|^2 = L \sum_{t, t'=0}^{2^n - 2} (-1)^{\text{tr}[(\alpha^\tau + 1)(\alpha^t + \alpha^{t'})]}$$

This can itself be written as

$$\sum_{k=0}^{2^n-2} |P(\tau, k, L)|^2 = L(2^n - 1) + L \sum_{0 \leq t \neq t' \leq 2^n-2}^{2^n-2} (-1)^{\text{tr}[(\alpha^\tau + 1)(\alpha^t + \alpha^{t'})]}$$

or

$$\sum_{k=0}^{2^n-2} |P(\tau, k, L)|^2 = (2^n - 1)L + L \sum_{u=1}^{2^n-2} \sum_{t=0}^{2^n-2} (-1)^{\text{tr}[(\alpha^\tau + 1)(\alpha^u + 1)\alpha^t]}$$

which gives $\sum_{k=0}^{2^n-2} |P(\tau, k, L)|^2 = (2^n - 1)L + L(L - 1)(-1)$ as required.

An exponential sum for Family A

The following result holds for both odd and even n :

Lemma 1 *Consider the sum defined as*

$$S(\gamma) = \sum_{x \in G_1} \omega^{T(\gamma x)}.$$

Then, for all ν in R^ we have*

$$\sum_{\gamma_i, \gamma_j \in \Gamma_\nu} \sum_{\tau=0}^{2^n-2} \mathcal{R} \{ S(\gamma_i \beta^\tau - \gamma_j) \} = 1.$$

Global Second Partial Correlation Function

Definition 4 We define the global (not for fixed τ) second partial correlation moment for family A as:

$$\langle |P(L)|^2 \rangle = \frac{1}{(2^{2n} - 1)^2} \sum_{k, \tau=0}^{2^n - 2} \sum_{\gamma_i, \gamma_j \in \Gamma_v} |P_{i,j}(\tau, k, L)|^2$$

Theorem 2 The global second partial correlation moment for Family A is given by

$$\langle |P(L)|^2 \rangle = L + \frac{L(L - 1)}{(2^{2n} - 1)^2}.$$

Proof

We have: $\sum_{k,\tau=0}^{2^n-2} \sum_{i,j=0}^{2^n} P_{i,j}(\tau, k, L) [P_{i,j}(\tau, k, L)]^*$ which can be rewritten as

$$\begin{aligned} & \sum_{t,\tau=0}^{2^n-2} \sum_{i,j=0}^{2^n} \sum_{k,l=0}^{L-1} \omega^{s_i(k \oplus t \oplus \tau) - s_j(k \oplus t) - s_i(l \oplus t \oplus \tau) + s_j(l \oplus t)} = \\ & = \sum_{i,j=0}^{2^n} \sum_{\tau=0}^{2^n-2} \sum_{k,l=0}^{L-1} \sum_{t=0}^{2^n-2} \omega^{T[(\beta^k - \beta^l)(\beta^\tau \gamma_i - \gamma_j)\beta^t]}. \end{aligned}$$

We now separate the case $k = l$, and note that we can use complex conjugate symmetry of the $(\beta^k - \beta^l)$ terms to rewrite the sum as:

$$\begin{aligned}
& L(2^n - 1) \left(\sum_{i,j=0}^{2^r} \sum_{\tau=0}^{2^n-2} 1 \right) + \\
& + \sum_{0 \leq k \neq l \leq L-1} \sum_{i,j,\tau} 2 \operatorname{Re} \{ S((\beta^k - \beta^l)(\beta^\tau \gamma_i - \gamma_j)) \} \\
= & L(2^{2n} - 1)^2 + 2 \sum_{0 \leq l < k \leq L-1} \sum_{i,j,\tau} \operatorname{Re} \{ S(\beta^\tau \gamma_i - \gamma_j) \}
\end{aligned}$$

where the argument of the sum $S(\cdot)$ simplifies since i is invariant under multiplication by a nonzero unit. Now note that the inner sum has been evaluated in Lemma 6 to observe that the sum becomes

$$L(2^{2n} - 1)^2 + 2[L(L - 1)/2] = L(2^{2n} - 1)^2 + L(L - 1)$$

and the result follows by normalization.

”Local” Partial Period Correlation for Family A

We are now ready to prove our “local” second moment for partial period correlations in *Family A*. This computes the average interference seen by sequence s_i .

Definition 5 *We define the local second partial correlation moment for Family A with respect to sequence s_i as:*

$$\left\langle |P(L)^{(i)}|^2 \right\rangle = \frac{1}{(2^n - 1)^2(2^n + 1)} \sum_{k, \tau=0}^{2^n-2} \sum_{\gamma_j \in \Gamma_v} |P_{i,j}(\tau, k, L)|^2$$

Classification of Family A Sequences

(a) $n = 2t + 1$ (an odd integer)		
<i>Subset</i>	\aleph	No. of Sequences
\mathcal{B}	-1	1
\mathcal{P}	$2^t - 1 + \omega 2^t$	$2^{t-1}(2^t + 1)$
\mathcal{Q}	$-2^t - 1 - \omega 2^t$	$2^{t-1}(2^t - 1)$
\mathcal{R}	$2^t - 1 - \omega 2^t$	$2^{t-1}(2^t + 1)$
\mathcal{S}	$-2^t - 1 + \omega 2^t$	$2^{t-1}(2^t - 1)$

The class containing the sequence s_i belongs to, determines its local second partial correlation moment.

Theorem 3 *Let n be odd. The local second partial correlation moment for sequence s_i in Family A is given by*

$$\left\langle |P(L)^{(i)}|^2 \right\rangle = L \pm \frac{L(L-1)2^{(n-1)/2}}{(2^n - 1)^2(2^n + 1)}.$$

where if $\gamma_i \in \mathcal{Q} \cup \mathcal{S}$ the second term is positive, and if $\gamma_i \in \mathcal{P} \cup \mathcal{R}$ the second term is negative.

Concluding remarks

- Partial Correlation properties were studied.
- Described first two moments of the function for Family A
- The results for Family B are much more complicated, see my paper with P. Udaya in SETA-08!