

AUTOCORRELATION FOR A CLASS OF POLYNOMIALS WITH COEFFICIENTS DEFINED ON T^*

M. TAGHAVI

Department of Mathematics, College of Sciences, Shiraz University, Shiraz, I. R. of Iran
 Email: taghavi@math.susc.ac.ir

Abstract – In this work we deal with the coefficients of $|A(e^{it})|^2$, where A is in a class of polynomials having Unimodular coefficients. We first present a technique that calculates lower bounds for particular autocorrelations and then in a more general case we present an upper bound for their maximal order.

Keywords – Autocorrelation, frequency, Fourier coefficient

1. INTRODUCTION

Let $A(z) = a_0 + a_1z + \dots + a_dz^d$ ($z \in C$) be a polynomial of degree d with complex coefficients. The coefficients of $A^2(z)$ are called the *correlations* of A and each of the $2d+1$ integers lying in the interval $[0, 2d]$ is called a *frequency* of $A^2(e^{it})$. For $k \in \{0, 1, \dots, d\}$ define $c_k = \bar{a}_0a_k + \bar{a}_1a_{k+1} + \dots + \bar{a}_{d-k}a_d$ and set $c_{-k} = \bar{c}_k$. The $2d+1$ complex numbers $c_{-d}, \dots, c_0, \dots, c_d$ are called the *autocorrelations* of A. The frequencies of the trigonometric polynomial $|A(e^{it})|^2$ are those integers in the interval $[-d, d]$.

As is mentioned in references [1] and [2], estimating the correlation and autocorrelation (in absolute value) of a polynomial with coefficients defined on the unit circle T is a useful tool in telecommunication. Most of the work was and still is to find the best upper bound at some class of frequencies and to find the lower bound at a given frequency. In [3] we used 2-stable cycle technique and estimated correlation of the Rudin-Shapiro polynomials at a particular frequency. In [4] we introduced a quite fast algorithm and calculated the autocorrelations numerically. In what follows we stay away from computers, and again present a new technique for estimating autocorrelations (in absolute value) of the Rudin-Shapiro polynomials.

Let $A(z) = a_0 + a_1z + \dots + a_dz^d$ and $B(z) = b_0 + b_1z + \dots + b_dz^d$ be polynomials such that their coefficients take only the values $+1$ or -1 . The pair $(A(z), B(z))$ of polynomials is said to have *Golay condition* if

$$|A(e^{it})|^2 + |B(e^{it})|^2 = 2d + 2. \quad (1)$$

In that case, the pair itself is called a *Golay polynomial pair*. Since the early 1950s Goley polynomials have been studied extensively by telecommunication engineers and their properties are provided in [5], [6] and [7]. Our main interest is on a type of Golay polynomial pair (p_n, q_n) inductively defined as follows: $(p_0, q_0) = (1, 1)$ and for any integer $n \geq 1$.

$$p_n(z) = p_{n-1}(z) + z^{L_{n-1}}q_{n-1}(z), \quad q_n(z) = p_{n-1}(z) - z^{L_{n-1}}q_{n-1}(z), \quad (2)$$

*Received by the editor March 15, 2006 and in final revised form August 13, 2007

where $L_n = 2^n$. They are called the Rudin-Shapiro polynomials and were introduced by H. S. Shapiro in 1951, [5]. To see if they are of Golay form, one can easily verify that.

$$p_n(z) = \varepsilon_0 + \varepsilon_1 z + \cdots + \varepsilon_{L_n-1} z^{L_n-1}, \quad q_n(z) = \delta_0 + \delta_1 z + \cdots + \delta_{L_n-1} z^{L_n-1},$$

where ε_k and δ_k take only the values +1 or -1.

Lemma 1. The Rudin-Shapiro polynomials have Golay condition.

Proof: Note that for $n \geq 0$, the degree of $p_n(z)$ and $q_n(z)$ are $L_n - 1$. Since $|p_0(e^{it})|^2 + |q_0(e^{it})|^2 = 1 + 1 = 2 = 2 \times 0 + 2$, we conclude that $(p_0(z), q_0(z))$ is a Golay polynomial pair. Suppose that for some $n \geq 0$, $(p_n(z), q_n(z))$ is a Golay polynomial pair. By (2),

$$\begin{aligned} |p_{n+1}(e^{it})|^2 &= \overline{p_n(e^{it})} e^{itL_n} q_n(e^{it}) + (|p_n(e^{it})|^2 + |q_n(e^{it})|^2) + p_n(e^{it}) \overline{e^{itL_n} q_n(e^{it})} \\ &= (|p_n(e^{it})|^2 + |q_n(e^{it})|^2) + 2\operatorname{Re}(e^{itL_n} p_n(e^{it}) q_n(e^{it})) \end{aligned}$$

and

$$\begin{aligned} |q_{n+1}(e^{it})|^2 &= -\overline{p_n(e^{it})} e^{itL_n} q_n(e^{it}) + (|p_n(e^{it})|^2 + |q_n(e^{it})|^2) - p_{n-1}(e^{it}) \overline{e^{itL_n} q_n(e^{it})} \\ &= (|p_n(e^{it})|^2 + |q_n(e^{it})|^2) - 2\operatorname{Re}(e^{itL_n} p_{n-1}(e^{it}) q_n(e^{it})). \end{aligned}$$

Hence, since $p_n(z)$ is of degree $L_n - 1$, by induction, we have

$$\begin{aligned} |p_{n+1}(e^{it})|^2 + |q_{n+1}(e^{it})|^2 &= 2[|p_n(e^{it})|^2 + |q_n(e^{it})|^2] \\ &= 2[2(L_n - 1) + 2] \\ &= 2(L_{n+1} - 1) + 2. \end{aligned}$$

Thus $(p_{n+1}(z), q_{n+1}(z))$ is a Golay polynomial pair. Therefore, the Rudin-Shapiro polynomials have Golay condition. That is,

$$|p_n(e^{it})|^2 + |q_n(e^{it})|^2 = 2^{n+1}. \quad (3)$$

2. A LOWER BOUND FOR AUTOCORRELATIONS

In what follows p_n and q_n are the Rudin-Shapiro polynomials and the variable z is restricted so that $|z| = 1$. For fixed n , the polynomial p_n is of degree $L_n - 1$ and so the frequencies of $|p_n|^2$, written $\operatorname{freq}(|p_n|^2)$, are integers in the frequency interval $[1 - L_n, L_n - 1]$. Also, since q_n is of degree $L_n - 1$, both $\operatorname{freq}(p_n \bar{q}_n)$ and $\operatorname{freq}(\bar{p}_n q_n)$ are integers in $[1 - L_n, L_n - 1]$. Let α_n be one of these frequencies and $g_n \in \{|p_n|^2, p_n \bar{q}_n, \bar{p}_n q_n\}$. By the *Fourier coefficient of g_n at α_n* we mean the coefficient for the term z^{α_n} , or simply

$$(g_n)^\wedge(\alpha_n) = \frac{1}{2\pi} \int_0^{2\pi} e^{-it\alpha_n} g_n(e^{it}) dt.$$

One can easily see that in the case $g_n = |p_n|^2$, there are $2^{n+1} - 1$ Fourier coefficients of g_n , which are actually the autocorrelations of p_n . Also, due to the restriction on z (that is $|z| = 1$),

$(z^{L_n-m} g_n)^{\wedge}(\alpha_n) = (g_n)^{\wedge}(\alpha_n - L_{n-m})$ for every integer m . We set $(g_n)^{\wedge}(\alpha_n) = 0$ anytime α_n lies outside of the interval $[1 - L_n, L_n - 1]$.

To see the location of frequencies at which the maximum autocorrelations occur, we start to examine the $2^2 \times 2^2$ square representation of $|p_2|^2$. It is formed by four 2×2 squares where each is formed by four squares as follows:

$$\bar{p}_2 \begin{array}{c} \begin{array}{cc} \overbrace{\quad\quad}^{p_2} \\ \underbrace{p_1} & \underbrace{q_1} \\ \underbrace{p_0} & \underbrace{q_0} \quad \underbrace{p_0} & \underbrace{-q_0} \end{array} \\ \begin{array}{|c|c|c|c|} \hline |p_0|^2 & \bar{p}_0 q_0 & |p_0|^2 & -\bar{p}_0 q_0 \\ \hline p_0 \bar{q}_0 & |q_0|^2 & p_0 \bar{q}_0 & -|q_0|^2 \\ \hline |p_0|^2 & \bar{p}_0 q_0 & |p_0|^2 & -\bar{p}_0 q_0 \\ \hline -p_0 \bar{q}_0 & -|q_0|^2 & -p_0 \bar{q}_0 & |q_0|^2 \\ \hline \end{array} \end{array}$$

For any $j, k \in \{1, 2, 3, 4\}$, we label value in the square located at j th row and k th column by $b_{j,k}$. In the above example, $b_{j,k} = \pm 1$ for all j and k . Although it is not our intention here, one use of this square representation is that, without calculating, we are able to write $|p_2(e^{it})|^2$ as

$$\begin{aligned} |p_2(e^{it})|^2 &= (b_{1,4})e^{3it} + (b_{1,3} + b_{2,4})e^{2it} + (b_{1,2} + b_{2,3} + b_{3,4})e^{it} \\ &\quad + (b_{1,1} + b_{2,2} + b_{3,3} + b_{4,4}) \\ &\quad + (b_{2,1} + b_{3,2} + b_{4,3})e^{-it} + (b_{3,1} + b_{4,2})e^{-2it} + (b_{4,1})e^{-3it} \\ &= -e^{3it} + e^{it} + 4 + e^{-it} - e^{-3it}. \end{aligned}$$

In general, one may represent $|p_n|^2$ by $2^n \times 2^n$ squares, each of which is formed by four $2^{n-1} \times 2^{n-1}$ squares and so on. The constant term of $|p_n(e^{it})|^2$ always equals 2^n and it is called the central coefficient. For the $n = 2$ case above, the length of all non central coefficients is 1. Therefore the maximum autocorrelation of p_2 is 1, but this is not so for $n \geq 3$. By presenting the square representation of $|p_4|^2$ the same as above, we noticed that it has maximum autocorrelation of length 5, and is the coefficient of the e^{11it} term (or to say at frequency 11). In $|p_6|^2$ and $|p_8|^2$ the maxima appear respectively at frequencies 43 and 171. Writing the binary representations for 11, 43 and 171 we get 1011 ($n = 4$), 101011 ($n = 6$) and 10101011 ($n = 8$). Hence we suspected that in a general case, anytime n is an even integer, the maximum would occur at 1010...1011 (n digits) and equals $\frac{1}{3}(2L_n + 1)$. The square representation of $|p_n|^2$ may also be presented as

$$\bar{p}_n \begin{array}{c} \begin{array}{cc} \overbrace{\quad\quad}^{p_n} \\ \underbrace{p_{n-1}} & \underbrace{q_{n-1}} \\ \underbrace{p_{n-2}} & \underbrace{q_{n-2}} \quad \underbrace{p_{n-2}} & \underbrace{-q_{n-2}} \end{array} \\ \begin{array}{|c|c|c|c|} \hline |p_{n-2}|^2 & \bar{p}_{n-2} q_{n-2} & |p_{n-2}|^2 & -\bar{p}_{n-2} q_{n-2} \\ \hline p_{n-2} \bar{q}_{n-2} & |q_{n-2}|^2 & p_{n-2} \bar{q}_{n-2} & -|q_{n-2}|^2 \\ \hline |p_{n-2}|^2 & \bar{p}_{n-2} q_{n-2} & |p_{n-2}|^2 & -\bar{p}_{n-2} q_{n-2} \\ \hline -p_{n-2} \bar{q}_{n-2} & -|q_{n-2}|^2 & -p_{n-2} \bar{q}_{n-2} & |q_{n-2}|^2 \\ \hline \end{array} \end{array}$$

and using this square, we write $|p_n(z)|^2$ in terms of $|p_{n-2}|^2$, $|q_{n-2}|^2$, $\bar{p}_{n-2} q_{n-2}$, and $p_{n-2} \bar{q}_{n-2}$ as follows:

$$\begin{aligned}
|p_n(z)|^2 &= (b_{1,4})z^{3L_{n-2}} + (b_{1,3} + b_{2,4})z^{2L_{n-2}} + (b_{1,2} + b_{2,3} + b_{3,4})z^{L_{n-2}} \\
&\quad + (b_{1,1} + b_{2,2} + b_{3,3} + b_{4,4}) \\
&\quad + (b_{2,1} + b_{3,2} + b_{4,3})\bar{z}^{L_{n-2}} + (b_{3,1} + b_{4,2})\bar{z}^{2L_{n-2}} + (b_{4,1})\bar{z}^{3L_{n-2}} \\
&= -z^{3L_{n-2}}\bar{p}_{n-2}q_{n-2} + z^{2L_{n-2}}(|p_{n-2}|^2 - |q_{n-2}|^2) + z^{L_{n-2}}p_{n-2}\bar{q}_{n-2} \\
&\quad + 2(|p_{n-2}|^2 + |q_{n-2}|^2) \\
&\quad + \bar{z}^{L_{n-2}}\bar{p}_{n-2}q_{n-2} + \bar{z}^{2L_{n-2}}(|p_{n-2}|^2 - |q_{n-2}|^2) - \bar{z}^{3L_{n-2}}p_{n-2}\bar{q}_{n-2},
\end{aligned}$$

and therefore by Lemma 1, for $|z|=1$

$$\begin{aligned}
|p_n(z)|^2 &= 2(z^{L_{n-1}} + \bar{z}^{L_{n-1}})|p_{n-2}|^2 - (z^{3L_{n-2}} - \bar{z}^{3L_{n-2}})\bar{p}_{n-2}q_{n-2} \\
&\quad + (z^{L_{n-2}} - \bar{z}^{3L_{n-2}})p_{n-2}\bar{q}_{n-2} - L_{n-1}(z^{L_{n-1}} + \bar{z}^{L_{n-1}}) + 2^n.
\end{aligned}$$

Hence if k_n is a non zero frequency of $|p_n|^2$, then

$$\begin{aligned}
(|p_n|^2)^\wedge(k_n) &= 2[(z^{L_{n-1}} + \bar{z}^{L_{n-1}})|p_{n-2}|^2]^\wedge(k_n) \\
&\quad + [(z^{L_{n-2}} - \bar{z}^{3L_{n-2}})p_{n-2}\bar{q}_{n-2}]^\wedge(k_n) \\
&\quad - [(z^{3L_{n-2}} - \bar{z}^{L_{n-2}})\bar{p}_{n-2}q_{n-2}]^\wedge(k_n).
\end{aligned} \tag{4}$$

Now let n be an even integer and put $k_n = \frac{1}{3}(2L_n + 1)$, which of course is in the frequency interval $[1 - L_n, L_n - 1]$. The right side of the above expression involves six different Fourier coefficients. In the first one

$$2(z^{L_{n-1}}|p_{n-2}|^2)^\wedge(k_n) = 2(|p_{n-2}|^2)^\wedge(k_n - L_{n-1}) = 2(|p_{n-2}|^2)^\wedge(k_{n-2}),$$

and this is because

$$k_n - L_{n-1} = \frac{1}{3}(2L_n + 1) - L_{n-1} = \frac{1}{3}2^{n+1} - 2^{n-1} + \frac{1}{3} = \frac{1}{3}[2(2^{n-2}) + 1] = k_{n-2}$$

Similarly, in the fifth term we have

$$(z^{3L_{n-2}}\bar{p}_{n-2}q_{n-2})^\wedge(k_n) = (\bar{p}_{n-2}q_{n-2})^\wedge(k_n - 3L_{n-2}) = (\bar{p}_{n-2}q_{n-2})^\wedge(k_{n-2} - L_{n-2}).$$

Finally the second, third, fourth, and sixth expressions in (4) are all zero, because first of all

$$\text{freq}(|p_{n-2}|^2), \text{freq}(p_{n-2}\bar{q}_{n-2}), \text{freq}(\bar{p}_{n-2}q_{n-2}) \in [1 - L_{n-2}, L_{n-2} - 1],$$

and therefore non of these four terms have frequencies in this interval. So putting $k'_n = k_n - L_n$ (clearly in the frequency interval), the relation (4) reads

$$(|p_n|^2)^\wedge(k_n) = 2(|p_{n-2}|^2)^\wedge(k_{n-2}) - (\bar{p}_{n-2}q_{n-2})^\wedge(k'_n). \tag{5}$$

Next we consider the representation for $\bar{p}_n q_n$,

$$\bar{p}_n$$

	$\overbrace{p_{n-1}}^{q_n}$		
	$\overbrace{q_{n-2}}^{-q_{n-1}}$	$\overbrace{-p_{n-2}}^{-q_{n-1}}$	$\overbrace{q_{n-2}}$
	$\overbrace{p_{n-2}}$	$\overbrace{q_{n-2}}$	
$ p_{n-2} ^2$	$\bar{p}_{n-2}q_{n-2}$	$- p_{n-2} ^2$	$\bar{p}_{n-2}q_{n-2}$
$p_{n-2}\bar{q}_{n-2}$	$ q_{n-2} ^2$	$-p_{n-2}\bar{q}_{n-2}$	$ q_{n-2} ^2$
$ p_{n-2} ^2$	$\bar{p}_{n-2}q_{n-2}$	$- p_{n-2} ^2$	$\bar{p}_{n-2}q_{n-2}$
$-p_{n-2}\bar{q}_{n-2}$	$- q_{n-2} ^2$	$p_{n-2}\bar{q}_{n-2}$	$- q_{n-2} ^2$

which gives us

$$\begin{aligned} \bar{p}_n(z)q_n(z) &= (b_{1,4})z^{3L_{n-2}} + (b_{1,3} + b_{2,4})z^{2L_{n-2}} + (b_{1,2} + b_{2,3} + b_{3,4})z^{L_{n-2}} \\ &\quad + (b_{1,1} + b_{2,2} + b_{3,3} + b_{4,4}) \\ &\quad + (b_{2,1} + b_{3,2} + b_{4,3})\bar{z}^{L_{n-2}} + (b_{3,1} + b_{4,2})\bar{z}^{2L_{n-2}} + (b_{4,1})\bar{z}^{3L_{n-2}} \\ &= z^{3L_{n-2}}\bar{p}_{n-2}q_{n-2} + z^{2L_{n-2}}(|q_{n-2}|^2 - |p_{n-2}|^2) \\ &\quad - z^{L_{n-2}}p_{n-2}\bar{q}_{n-2} + \bar{z}^{L_{n-2}}(2p_{n-2}\bar{q}_{n-2} \\ &\quad + \bar{p}_{n-2}q_{n-2}) + \bar{z}^{2L_{n-2}}(|p_{n-2}|^2 - |q_{n-2}|^2) - \bar{z}^{3L_{n-2}}p_{n-2}\bar{q}_{n-2}. \end{aligned}$$

In a similar fashion as obtaining (5), we calculate the Fourier coefficient of $\bar{p}_n q_n$ at the frequency k'_n and get

$$(p_n \bar{q}_n)^\wedge(k'_n) = -2(|p_{n-2}|^2)^\wedge(k_{n-2}) + 2(\bar{p}_{n-2} q_{n-2})^\wedge(k'_{n-2}) + (p_{n-2} \bar{q}_{n-2})^\wedge(k'_{n-2}), \quad (6)$$

on which suggests that the Fourier coefficient of $p_n \bar{q}_n$ at k'_n is also needed. From the square representation of $p_n \bar{q}_n$ we obtain

$$(p_n \bar{q}_n)^\wedge(k'_n) = 2(|p_{n-2}|^2)^\wedge(k_{n-2}) + 2(\bar{p}_{n-2} q_{n-2})^\wedge(k'_{n-2}) + (p_{n-2} \bar{q}_{n-2})^\wedge(k'_{n-2}). \quad (7)$$

Let $w_n = \left[(|p_n|^2)^\wedge(k_n), (\bar{p}_n q_n)^\wedge(k'_n), (p_n \bar{q}_n)^\wedge(k'_n) \right]^T$ and A be a 3×3 matrix with entries 2, -1, 0, -2, 2, -1, 2, 2, 1 (started from first row). By (5), (6) and (7) we have $w_n = Aw_{n-2}$. Since this holds for any positive even integers, $w_n = Aw_{n-2} = A^2 w_{n-4} = \dots = A^{n/2} w_0$, where $w_0 = [1, 1, 0]^T$. If g is the characteristic polynomial of A , then $g(\lambda) = \lambda^3 - 5\lambda^2 + 12\lambda - 16$. g has three distinct non zero roots with one real and two non real. Let λ_1, λ_2 and λ_3 be the eigenvalues of A on which we may assume that the value on $|\lambda_1|$ is larger than both $|\lambda_2|$ and $|\lambda_3|$. These eigenvalues being distinct yields the existence of a nonsingular matrix S such that $S^{-1}AS = \Lambda$, where $\Lambda = \text{diag}[\lambda_1, \lambda_2, \lambda_3]$. Since $A^{n/2} = SA^{n/2}S^{-1}$, we have $w_n = A^{n/2}w_0 = SA^{n/2}S^{-1}w_0$. Therefore, there are constants a, b and c such that

$$\left(|p_n|^2 \right)^\wedge(k_n) = a\lambda_1^{n/2} + b\lambda_2^{n/2} + c\lambda_3^{n/2}. \quad (8)$$

Evaluating λ_1 and the constant a in (8), we get $|\lambda_1| = 2^{1.46}$ and $a=0.42$. So we have the existence of a constant $B > 0$ such that $\left(|p_n|^2 \right)^\wedge(k_n) > B|\lambda_1|^{n/2}$, the existence of an absolute constant B so that

$$\left(|p_n|^2 \right)^\wedge\left(\frac{1}{3}(2L_n + 1) \right) > BL_n^{0.73}. \quad (9)$$

If n is an odd integer, then we put $k_n = \frac{1}{3}(L_n + 1)$, and with similar calculations we get the same estimate.

We complete our discussion by presenting an upper bound for autocorrelations of the Rudin-Shapiro polynomials. In connection with choosing a particular frequency, it will be more general than our lower bound result.

Theorem: Suppose the f_n is $|p_n|^2$ or $|q_n|^2$, where (p_n, q_n) is the Rudin-Shapiro polynomial pair. Then

$$\max_{k \neq 0} (f_n)^\wedge(k) > \frac{1}{\sqrt{6}} L_n^{\frac{1}{2}}$$

Proof: By (2) we have

$$f_n(z) = \sum_{k=-(L_n-1)}^{k=L_n-1} d_k z^k.$$

Clearly $d_0 = L_n$ and so

$$\|f_n\|_2^2 = \frac{1}{2\pi} \int_0^{2\pi} |f_n(e^{it})|^2 dt = L_n^2 + 2 \sum_{k=1}^{L_n-1} |d_k|^2. \quad (10)$$

Also, note that

$$\frac{4}{3} - \frac{1}{2L_n} < \frac{\|f_n\|_2^2}{L_n^2} < \frac{4}{3} + \frac{1}{2L_n}. \quad (11)$$

This relation can easily be verified by an induction argument. Therefore (10), together with (11) imply that

$$\sum_{k=1}^{L_n-1} |d_k|^2 = \frac{1}{2} [\|f_n\|_2^2 - L_n^2] > \frac{1}{6} L_n^2 - \frac{1}{4} L_n.$$

Thus

$$\max_{k \neq 0} (f_n)^\wedge(k) = \sqrt{\max_{k \neq 0} |d_k|^2} \geq \sqrt{\frac{1}{L_n-1} \sum_{k=1}^{L_n-1} |d_k|^2} > \sqrt{\frac{2L_n^2 - 3L_n}{12(L_n-1)}} > \frac{1}{\sqrt{6}} L_n^{\frac{1}{2}}.$$

REFERENCES

1. Barker, R. H. (1953). *Group synchronizing of binary digital system*, in "Communication Theory", London, Butterworth.
2. Golay, M. J. (1949). on multislit spectrometry and applications. *Journal of Optical Society of America*.
3. Taghavi, M. (1996). An estimate on the correlation coefficients of the Rudin-Shapiro polynomials. *IJST*, 20(2), 235-240.
4. Abdolahi, A. & Taghavi, M. (2005). Dyadic representation of the Rudin-Shapiro Coefficients with applications. *J. Appl. Math. & Comp.*, 18(1-2), 301-310.
5. Shapiro, H. S. (1951). Extremal problems for polynomials and power series, Thesis, M.I.T.
6. Turyn, R. (1968). *Sequences with small correlation*, in "error correcting codes" (H. Mann editor), Wiley.
7. Schroeder, M. R. (1984). *Number Theory in Science and Communication*. Berlin Heidelberg, Springer-verlag.