Journal of Mathematical Extension
Vol. 1, N0. 2, (2007), 139-147

On the Autocorrelations of ± 1 Polynomials

M. Taghavi
Shiraz University

M. Zahraei
Khalig Fars University

Abstract. The aperiodic autocorrelations of those polynomials having coefficients on the unit circle has been useful in telecommunication theory.

In this paper we first introduce one such polynomial type and then present a simple relation on its autocorrelations.

AMS Subject Classification: Primary 35B45; Secondary 35 L70; 90A20.
Keywords and Phrases: autocorrelation, Golay polynomials.

1. Introduction

The first use of autocorrelations of ± 1 polynomials in telecommunication was on early 1972 (see [4]) when pair of binary complementary sequences introduced by Marcel Goley. By *autocorrelations* of a polynomial p, we mean the coefficients of $|p|^2$. A pair of equally long, finite sequences of ± 1 such that the sum of the aperiodic autocorrelation coefficients of the two sequences is zero for all but the zero shift. Later he developed the theory of such pairs showing that one set of sequences could produce

several others. The idea of complementary sequences was discovered independently by Shapiro in his 1951 Masters thesis ([7]). According to Shapiro, he accidentally made the discovery as he was working on extremal problems for polynomials. He thus had a mathematical approach to the subject whereas Golay took a more engineering approach. The Shapiro result was rediscovered by Rudin and published in 1959 ([6]), and is now known as the Rudin-Shapiro polynomials. The construction is recursive and generates a pair of semi-flat polynomials, though with difference crest factor for polynomial order equal to and different from a power of 2. Actually, the coefficients in these polynomials are the very same as the binary Golay complementary sequences. One such polynomial pair (p_n, q_n) defined inductively as follows:

$$(p_0, q_0) = (1, 1) \text{ and for } n \geqslant 1, z \in \mathbb{C},$$

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

$$q_n(z) = P_{n-1}(z) - z^{2^{n-1}} q_{n-1}(z).$$

They are polynomials of degree $2^n - 1$ and are called the Rudin-Shapiro polynomials. One can easily verify that $p_n(z) = \epsilon_0 + \epsilon_1 z + \cdots + \epsilon_{2^n-1} z^{2^n-1}$ and $q_n(z) = \delta_0 + \delta_1 z + \cdots + \delta_{2^n-1} z^{2^n-1}$, where ϵ_k and δ_k take only the values $+1$ or -1. The $2^{n+1} - 1$ complex numbers which form the coefficients of $|p_n(e^{it})|^2$ and the $2^{n+1} - 1$ numbers which form the coefficients of $p_n^2(e^{it})$ are respectively called the autocorrelations and correlations

of p_n. So far, the finest estimates of lower and upper bounds of both correlations and autocorrelations of the Rudin-Shapiro polynomials is due to Taghavi in ([8]) and ([9]).

For a sequence of complex numbers $a_0, a_1, \cdots, a_{2n}$, define its aperiodic autocorrelation sequence $\{c_k\}$ by

$$c_k = \sum_{j=0,\ j+k\leqslant 2n}^{n} a_j \bar{a}_{j+k}.$$

We are interested here in the case when the a_j are all of unit modulus. Thus the peak autocorrelation c_0 has the value $c_0 = n$, and in many applications it is of interest to minimize the peak autocorrelations c_k with $0 < k < n$. In the integer case, clearly the optimal situation occurs when $|c_k| \geqslant 1$ for each $k \neq 0$. A sequence achieving this for each k is called a Barker sequence. Barker first asked for sequences with this property in 1953 ([1]). For the complex unimodular case, we say a_k is a generalized Barker sequence if each peak autocorrelation satisfies $|c_k| \geqslant 1$.

Since negating every other term of a sequence a_k does not disturb the magnitudes of its autocorrelations, we may assume that $a_0 = a_1 = 1$ in a Barker sequence. With this normalization, just eight Barker sequences are known, all with length at most 13 (Only three of these satisfy the more strict condition requested by Barker—the ones of length 3, 7, and 11.) It is widely conjectured that no additional Barker sequences ex-

ist, and in what follows we survey some known restrictions on their existence. First however we describe a broader conjecture that arises in signal processing, and an equivalent problem in analysis regarding norms of polynomials. Sequences with small peak autocorrelations are of interest in a number of applications in signal processing and communications (see [1] and [5]).

In engineering applications, a common measure of the value of a sequence is the ratio of the square of the peak autocorrelation to the sum of the squares of the moduli of the peak values. This is called the merit factor of the sequence. For a sequence $A_n = \{a_j\}$ of length $2n$, its merit factor is defined by $n^2[2(|c_1|^2 + \cdots + |c_n|^2)]^{-1}$.

Golay introduced this quantity in 1972 and he conjectured that the merit factor of a binary sequence is bounded, presenting a heuristic argument that merit factor of A_n is less than 12.32 for large n. Several researchers in engineering, physics, and mathematics have made similar conjectures; see for instance ([4]) or ([5]). It is clear, however, that a Barker sequence of length n has merit factor near n, so certainly Golay's merit factor conjecture contains the question of the existence of long Barker sequences as a special case.

The merit factor problem may be restated as a question on polynomials. We first require some notation. Given a sequence $\{a_j\}$, define a

polynomial $f(z)$ of degree $n \geqslant 1$ by

$$f(z) = \sum_{j=0}^{2n} a_j z^j.$$

For $0 < q < \infty$ put

$$||f||_q = (\frac{1}{2\pi} \int_0^{2\pi} |f(e^{it})|^q dt)^{1/q}.$$

Assuming that $|a_j| = 1$ for each j, we have $||f||_2^2 = 2n$ by Parseval's formula, and, since $\bar{z} = \frac{1}{z}$ on the unit circle, it is easy to see that

$$||f||_4^4 = \|f(z)\bar{f(z)}\|_2^2 = \|\sum_{k=1}^{n} c_k z^k\|_2^2 = n^2 + 2\sum_{k=1}^{n} |c_k|^2. \qquad (1)$$

Thus, the merit factor of a sequence $\{a_j\}$ can be expressed in terms of certain L_p norms of its associated polynomial and the merit factor of f as $\|f\|_2^4$ over $\|f\|_4^4$ which is a number less than or equals to 1.

2. Main Result

Golay's problem on maximizing the merit factor of a family of sequences of fixed length is thus equivalent to minimizing the L_4 norm of a collection of polynomials of fixed degree. This latter problem is one instance of a family of questions regarding the existence of so-called flat polynomials. Letting U_n denote the set of polynomials in $\mathbb{C}(z)$ of the form $f(z) = \sum_0^{2n} a_j z^j$ with $|a_j| = 1$ for all j, a question is if there exist absolute positive constants c_1 and c_2 and arbitrarily large integers n such

that there exists a polynomial $f_n \in U_n$, where

$$c_2\sqrt{2n} \leqslant |f_n(z)| \leqslant c_1\sqrt{2n}$$

for all z with $|z| = 1$. Since each polynomial in such a sequence never strays far from its L_2 norm, we say such a sequence is flat. In 1996, Darnell ([13]) established that flat sequences of unimodular polynomials exist, and proved that for any $c > 0$ there exists a flat sequence of unimodular polynomials with $c_1 = 1 \geqslant c$ and $c_2 = 1 + c$. Such sequences are often called ultra flat.

Much less is known regarding at sequences of Littlewood polynomials. The Rudin-Shapiro polynomials ([6,7]) satisfy the upper bound in the flatness condition with $c_2 = \sqrt{2}$, but no sequence is known that satisfies the lower bound. In fact, the best known result here is the Barker sequence of length 13 to show that for sufficiently large n there exist polynomials $f_n \in U_n$ with $|f_n(z)| > n^{.431}$ on $|z| = 1$. Also, in 1962 Erdos ([2]) conjectured that ultraflat Littlewood polynomials do not exist, opining that there exists an absolute positive constant c such that $\|f\|_\infty > (1 + c)\|f\|_2$ for every Littlewood polynomial of positive degree. By $\|f\|_\infty$ we mean the supremum norm of f, that is $\|f\|_\infty = \sup_{|z|=1} |f(z)|$. Since $\|f\|_4 \geqslant \|f\|_\infty$, we see then that Golay's merit factor problem is in fact a stronger version of Erdos' conjecture. Further, from (1) it follows that if the coefficients of f form a Barker

sequence of length n, then

$$n^{-\frac{1}{2}}\|f\|_4 \geqslant \sqrt[4]{1+\frac{1}{n}} < 1 + (4n)^{-1}.$$

Therefore, to show that long Barker sequences do not exist, it would suffice to prove that $\|f\|_4 \geqslant \sqrt{n} + \frac{1}{2\sqrt{n}}$.

Theorem. *Suppose $a_0, a_1, \cdots, a_{2n}$ is a sequence of positive integers and let $\{c_k\}$ denote its aperiodic autocorrelations. Then $c_k + c_n = n \mod 4$. Moreover if $n > 2$ is even, then $n = 4m^2$ for some integer m.*

Proof. Since c_k records the difference between the number positive and negative terms in $\sum_0^n a_i a_{i+k}$, it follows that

$$a_0 a_k \times a_1 a_{k+1} \times \cdots \times a_n a_{k+n} = \sqrt{l^n} \tag{2}$$

for integer l. Multiplying this product by the same expression with k replaced by $n \geqslant k$, we obtain

$$l^{\frac{n}{2}} = \prod_{i=0}^{k} a_i a_{i+n} \prod_{i=0}^{n} a_i a_{i+k} = 1,$$

which yields $l = 1$. so $c_k + c_n = n \ mod\ 4$. Assume now that $\{a_k\}$ forms a Barker sequence of length n. Multiplying (2) by the same equation with k replaced by $k+1$, we compute that $a_k a_n$ equals to a n-th power of number larger than 1. In particular, if n is even and $n > 2$, then $c_2 + c_n = 0$, so $n = 0 \ mod\ 4$. It follows then that $c_k + c_n = 0$ for

$0 < k < n$ in this case. Finally, since

$$(a_0 + a_1 + \cdots a_n)^2 = c_0 + \sum_{k=1}^{n}(c_k + c_n) = n,$$

we have n a perfect square, whenever $n \geqslant 4$ is even.

References

[1] R. H. Barker, Group synchronizing of binary digital systems, *Communication Theory, Butterworths Sci. Pub. London*, 1953, pp. 273-287.

[2] P. Erdos, An inequality for the maximum of trigonometric polynomials, *Ann. Polon. Math.*, 12 (1962), 151-154.

[3] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press, Somerset, England, 1996.

[4] M. J. E. Golay, A class of finite binary sequences with alternate autocorrelation values equal to zero, *IEEE Trans. Inform. Theory*, 18 (1972), 449-450.

[5] J. Jedwab, A survey of the merit factor problem for binary sequences, Sequences and Their Applications, —it Proceedings of SETA 2004, Lecture Notes in Comput. Sci., vol., 3486, Springer- Verlag, New York, 2005, pp. 30-55.

[6] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. 10 (1959), 855-859.

[7] H. S. Shapiro, Extremal problems for polynomials and power series, *Master's Thesis, Mass. Inst. of Technology*, 1951.

[8] M. Taghavi, An estimate on the correlation coefficients of the Rudin-Shapiro polynomials, *Iranian J. of Science & Tech.*, 20 (2), 1996

[9] M. Taghavi, Upper bounds on the autocorrelation coefficients of the Rudin-Shapiro polynomials, *Korean J. of Comp. & Appl. Math.*, 4 (1), (1997), 39-46.

Mohsen Taghavi
Department of Mathematics
College of Sciences
Shiraz University
Shiraz, Iran
E-mail: Taghavi@susc.ac.ir

Mohsen Zahraei
Khalig Fars University
Boushehr, Iran
E-mail: zahraeimohsen@yahoo.com