Almost Perfect Binary Functions

Philippe Langevin
G.E.C.T. Université de Toulon, F-83130 La Garde, France

Received October 30, 1991; revised version August 5, 1992

Abstract. The almost perfect binary sequences have been defined in [6] as \((-1, +1)\)-periodic sequences such that all their out-of-phase autocorrelation coefficients are zero except one. In the preceding paper, the study of the almost perfect binary sequences is done by means of the ring \(\mathbb{F}_2[X]/(X^n - 1)\). Here, the arithmetic of cyclotomic fields enables us to solve open problems and questions like: structure and existence of these sequences.

Keywords: Correlation, Sequences, Fourier transform

In what follows, we identify the periodic sequences of length \(n\) with the mapping defined over \(\mathbb{Z}/n\mathbb{Z}\), so that we use the notation \(i \rightarrow s(i)\) for the sequence \(s_0, s_1, \ldots, s_{n-1}\). By “binary” function (or sequence), we understand a map with codomain \([-1, +1] \subset \mathbb{C}\). For any trouble with notations, one may refer to section 8.

1. Almost Perfect Function

Let \(n\) be an integer. A map \(f\) from \(\mathbb{Z}/n\mathbb{Z}\) into \(\mathbb{C}\) is said to be \(D\)-perfect, if:

\[ f \times f(z) = 0, \quad \forall z = 1, 2, \ldots, D - 1 \]

where \(f \times f(z) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} f(x)f(x + z)\) is the autocorrelation function of \(f\).

The \(n\)-perfect functions whose codomain is the set of \(n\)th-root of unity, are the generalized bent functions of dimension one – see [4] – and can be obtained via Gauss sums. The set of \(n\)-perfect binary functions is in one to one correspondance with the set of the Hadamard circulant matrix, and thus – see [1, Chap. 4] – when \(4 < n \leq 12100\), there are no \(n\)-perfect binary functions, so that the greatest \(D\) for which one may find \(D\)-perfect functions becomes \(n/2\) – see [6]. These functions are called almost perfect (binary) functions.
**Proposition 1.** If \( f \) is an almost perfect function of length \( n \) then

(i) \( n \) is a multiple of \( 4 \)

(ii) \( f \times f(z) = \begin{cases} n, & \text{if } z = 0; \\ \hat{f}(0)^2 - n, & \text{if } z = n/2; \\ 0, & \text{else.} \end{cases} \)

where \( \hat{f}(0) \) is the Fourier transform, see further, of \( f \) at \( 0 \) and must be even.

**Proof.** See [6, Proposition 1 and Corollary 6]. \( \square \)

The almost perfect functions with \( f \times f(n/2) \leq 0 \) are of a great interest for synchronization problems. When \( n \geq 8 \), one only knows the experimental results of J. Wolfmann which all have \( \hat{f}(0) \) equal to 2 or 4.

### 2. Algebraic Preliminaries

Let \( \zeta_n \) be a primitive \( n \)-th root of unity in \( \mathbb{C} \). The ring of integers of \( \mathbb{Q}(\zeta_n) \) is \( \mathbb{Z} [\zeta_n] \) – see [2]. If \( p \) is a prime, we denote by \( G_n(p) \) the decomposition group of \( p \), and by \( e_n(p), f_n(p), g_n(p) \) the index, the degree, and the order of ramification of \( p \). The group \( (\mathbb{Z}/n\mathbb{Z})^* \) is isomorphic to \( \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \) by means of \( q \mapsto \sigma_q \), where \( \sigma_q \) is defined by the action \( \zeta_n \mapsto \zeta_n^q \). The ideal \( (p) \) is equal to \( \prod_{i=1}^{e_n(p)} P_i^{f_n(p)} \), where the \( P_i \) are distinct prime ideals containing \( (p) \) fixed by \( G_n(p) \). \( f_n(p) \) is the common degree of the algebraic extension \( \mathbb{Z} [\zeta_n]/P_i \) of \( \mathbb{Z}/p\mathbb{Z} \) and the equality \( e_n(p)f_n(p)g_n(p) = \phi(n) \) holds. Moreover, if \( p \) does not divide \( n \) then \( e_n(p) = 1 \) and \( G_n(p) \) is cyclic generated by \( \%_p \).

**Lemma 2.** Let \( a \) be a positive integer whose decomposition in prime factors is

\[
a = \prod_{\mathfrak{p}|a} p^{v_{\mathfrak{p}}(a)}
\]

If there exists \( p \) such that \( \sigma^{-1} \in G_n(p) \) and \( e_n(p)r_p \) is odd, then the equation \( z \bar{z} = a \) has no solution in \( \mathbb{Z} [\zeta_n] \).

**Proof.** Let \( z \) an algebraic integer such that \( z \bar{z} = a \) and \( p \) a prime ideal containing \( (p) \). The valuation \( v_{\mathfrak{p}}(z) \) of \( (z) \) is equal to \( v_{\mathfrak{p}}(\bar{z}) \), thus the \( \pi \)-adic valuation of \( a \), that is \( e_n(p)r_p \), must be even. \( \square \)

**Lemma 3.** Let \( a \) be a positive integer, \( z \in \mathbb{Z} [\zeta_n] \) and \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \) such that \( z \bar{z} = a \) and \( \sigma \in \bigcap_{\mathfrak{p}|a} G(p) \) then there exists a root of unity \( \lambda \) such that \( \sigma(z) = \lambda z \).

**Proof.** Let \( z \) an algebraic integer such that \( z \bar{z} = a \). The principal ideal \( (z) \) is a product of prime ideals containing \( a \). Each of them is fixed by \( \sigma \), thus \( (z) \) and \( (\sigma(z)) \) are equal. There exists an unit \( \lambda \) such that \( \sigma(z) = \lambda z \). On an other hand,