# On a hierarchy of Boolean functions hard to compute in constant depth

Anna Bernasconi

*Discrete Mathematics and Theoretical Computer Science* **4**, 2001, 79–90

# *On a hierarchy of Boolean functions hard to compute in constant depth*†

Anna Bernasconi

*Dipartimento di Informatica, Università degli Studi di Pisa, Corso italia, 40, 56125 Pisa, Italy.*
*e-mail:* `annab@di.unipi.it`

*received March 1999, revised July 2000, accepted March 2001.*

Any attempt to find connections between mathematical properties and complexity has a strong relevance to the field of Complexity Theory. This is due to the lack of mathematical techniques to prove lower bounds for general models of computation.

This work represents a step in this direction: we define a combinatorial property that makes Boolean functions "hard" to compute in constant depth and show how the harmonic analysis on the hypercube can be applied to derive new lower bounds on the size complexity of previously unclassified Boolean functions.

**Keywords:** Boolean functions, $AC^0$ circuits, size complexity, harmonic analysis

## 1 Introduction

Any attempt to find connections between mathematical properties of functions and their computational complexity has a strong relevance to theory of computation. Indeed, there is the hope that developing new mathematical techniques could lead to discovering properties that might be responsible for lower bounds. The subject of this paper is related to the above general arguments, and in particular to showing how the Abstract Harmonic Analysis on the hypercube can provide some insight in our current understanding of Boolean function complexity. Our main result consists of new lower bounds on the size complexity of explicit functions, exactly derived by applying the above techniques.

One of the best-known results in Circuit Complexity is that constant depth circuits require exponential size to compute the parity function (see [4, 5, 11]). Here we generalize this result to a new hierarchy of functions.

This hierarchy is defined as follows. Let $p$ be a positive rational number, $0 < p \leq 1$, and let $\mathcal{B}_n^{(p)}$ be the class of functions, depending on $n$ variables, that take the value 1 with probability $p$, i.e. on exactly $2^n p$ input strings.

†A preliminary version of this paper was published in *Proceedings of the 4th International Computing and Combinatorics Conference* (COCOON'98), Lectures Notes in Computer Science 1449, 1998.

We then divide $\mathcal{B}_n^{(p)}$ into *levels*, where the $k$-th level, which we denote by $B^{(p,k)}$, is defined as the subset of the functions $f \in \mathcal{B}_n^{(p)}$ such that any subfunction of $f$, depending on $k$ ($k \geq \log \frac{1}{p}$) variables, takes the value 1 again with probability $p$, i.e. on $2^k p$ input strings (w.l.o.g. let us assume that $2^k p$ is an integer). These definitions are made precise below.

Our main result is that $AC^0$-circuits cannot compute functions in the $k$-th level of $\mathcal{B}_n^{(p)}$, whenever

$$k = n - (\log n)^{\omega(1)}$$

and

$$p = \Omega(2^{-\mathrm{polylog}\, n}).$$

More precisely, we prove that a circuit of constant depth $d$ require size

$$\Omega\left(2^{\frac{(n-k)^{1/d}}{20}}\, p\right)$$

to compute any function in $B^{(p,k)}$, for any $p$ and any $k$.

We also prove that nontrivial functions exist for each level of this hierarchy if

$$k > \frac{\log p + 1}{\log p}\, n,$$

and conjecture that this bound is not far from being asymptotically optimal.

The main tool of the lower bound proof is the harmonic analysis on the hypercube, that yields an interesting spectral characterization of the functions in the above hierarchy, together with a result proved in [8], stating that $AC^0$ functions have almost all of their *power spectrum* on the low-order coefficients.

Finally, notice that this paper generalizes results in [1], where it has been proven that $AC^0$-circuits cannot compute *strongly balanced functions*. Indeed, the class of strongly balanced functions coincides with the $\left[n - (\log n)^{\omega(1)}\right]$-th level of the class $\mathcal{B}_n^{(1/2)}$.

The results presented in this paper have recently been improved in [3, 2], where it is shown how this spectral technique for proving lower bounds on the size-complexity of Boolean functions can be generalized in order to be applied also to functions which present the combinatorial structure described above only in an "approximate sense". In this way some new interesting lower bounds have been obtained for functions related to some arithmetic properties of integers. Precisely it has been shown that deciding if a given integer is square-free and testing co-primality of two integers by unbounded fan-in circuits of bounded depth requires superpolynomial size (the number theoretic counterpart of the spectral technique is a sieve method).

The rest of the paper is organized as follows. In Section 2 we provide some of the notation we use, and recall some basic definitions. In Section 3 we give the necessary background on Fourier transform on the hypercube, and review the results by Linial et al. [8] about the spectral characterization of $AC^0$ functions. Section 4 is devoted to the definition of the classes $\mathcal{B}_n^{(p)}$ and of their levels $B^{(p,k)}$. In Section 5 we derive a spectral characterization of the functions in any level of $\mathcal{B}_n^{(p)}$, and in Section 6 we prove our main result stating that $AC^0$-circuits cannot compute functions in the level $B^{(p,k)}$, whenever $k = n - (\log n)^{\omega(1)}$ and $p = \Omega(2^{-\mathrm{polylog}\, n})$. In Section 7 we prove that nontrivial functions do exist in any level $B^{(p,k)}$ such that $k > \frac{\log p+1}{\log p}\, n$. Finally, in Section 8 we provide a framework for future research.

## 2 Basic Definitions

First of all, we provide some of the notation we use.

Given a Boolean function $f$ on $n$ binary variables, we will use different kinds of notation: the *classical notation*, where the input string is given by $n$ binary variables; the *set notation*, based on the correspondence between the set $\{0,1\}^n$ and the power set of $\{1,2,\dots,n\}$; the $2^n$-tuple *vector representation* $f = (\, f_0\, f_1 \dots f_{2^n-1}\,)$, where $f_i = f(x(i))$ and $x(i)$ is the binary expansion of $i$. Unless otherwise specified, the indexing of vectors and matrices starts from 0 rather than 1.

We will use the notation $|f|$ to denote the *cardinality* of $f$, that is the number of strings accepted by $f$:

$$|f| = |\{w \in \{0,1\}^n \mid f(w) = 1\}|\,.$$

Given a binary string $w \in \{0,1\}^n$, we denote with $w^{(i)}$ the string obtained from $w$ by flipping its $i$-th bit ($1 \le i \le n$), i.e. $w$ and $w^{(i)}$ differ only on the $i$-th bit, and by $|w|_1$ the *hamming weight* of $w$, i.e. the number of ones in it. If $w$ and $v$ are two binary strings of the same length, then $w \oplus v$ denotes the string obtained by computing the *exclusive or* of the bits of $w$ and $v$. Finally, all the logarithms are to the base 2, and the notation polylog $n$ stands for a function growing like a polynomial in the logarithm of $n$.
We now review some basic definitions.

**$AC^0$ circuits**

An $AC^0$ circuit consists of AND, OR and NOT gates, with inputs $x_1,\dots,x_n$. Fan-in to the gates is unbounded. The size of the circuit (i.e. the number of the gates) is bounded by a polynomial in $n$, and its depth is bounded by a constant. Without loss of generality we can assume that negations occur only as negated input variables. If negations appear higher up in the circuit we can move them down to the inputs using De Morgan's laws which at most doubles the size of the circuit. Finally, observe that we have alternating levels of AND and OR gates, since two adjacent gates of the same type can be collapsed into one gate (for a more detailed description, see [5]).

**Restriction**

A *restriction* $\rho$ is a mapping of the input variables to the set $\{0,1,\star\}$, where

- $\rho(x_i) = 0$ means that we substitute the value 0 for $x_i$;
- $\rho(x_i) = 1$ means that we substitute the value 1 for $x_i$;
- $\rho(x_i) = \star$ means that $x_i$ remains a variable.

Given a function $f$ on $n$ binary variables, we will denote by $f_\rho$ the function obtained from $f$ by applying the restriction $\rho$; $f_\rho$ will be a function of the variables $x_i$ for which $\rho(x_i) = \star$.

The *domain* of a restriction $\rho$, $dom(\rho)$, is the set of variables mapped to 0 or 1 by $\rho$. The *size* of a restriction $\rho$, $size(\rho)$, is defined as the number of variables which were given the value $\star$, i.e. $size(\rho) = n - |dom(\rho)|$.

## 3 Abstract Harmonic Analysis and $AC^0$ Functions

We give some background on abstract harmonic analysis on the hypercube. We refer to [7] for a more detailed exposition.

We consider Boolean functions as embedded in the space $\mathcal{F}$ of all real-valued functions on the domain $\{0,1\}^n$. On $\mathcal{F}$ we consider the standard scalar product

$$\langle f,g\rangle = \frac{1}{2^n} \sum_{w\in\{0,1\}^n} f(w)g(w) \tag{1}$$

with induced norm $\|f\| = \langle f,f\rangle^{1/2}$.

The functions $Q_w(x) = (-1)^{w_1x_1}(-1)^{w_2x_2}\dots(-1)^{w_nx_n} = (-1)^{w^Tx}$ are known as **Fourier transform kernel functions**, and the set

$$\{Q_w \,|\, w \in \{0,1\}^n\}$$

is an orthogonal basis for $\mathcal{F}$.

We can now define the *Abstract Fourier Transform* of a Boolean function $f$ as the rational valued function $\hat{f}$ which defines the coordinates of $f$ with respect to the basis $\{Q_w(x)\,|\,w \in \{0,1\}^n\}$, i.e.,

$$\hat{f}(w) = \frac{1}{2^n} \sum_x Q_w(x) f(x)\,. \tag{2}$$

Then

$$f(x) = \sum_w Q_w(x) \hat{f}(w) \tag{3}$$

is the Fourier expansion of $f$.

It is interesting to note that the zero-order Fourier coefficient is equal to the probability that the function takes the value 1, while the other Fourier coefficients measure the correlation between the function and the parity of subsets of its input bits. This is immediate to see if the Boolean functions are defined as mapping from $\{0,1\}^n$ to $\{1,-1\}$, where $-1$ stands for "accept" and 1 stands for "reject" (see [8] for more details), but remains of course true even for $\{0,1\}$-valued functions (the coefficients of order greater than zero differ in the two cases only by a constant factor).

Using the binary $2^n$-tuple representation for the functions $f$ and $\hat{f}$, and considering the natural ordering of the $n$-tuples $x$ and $w$, one can derive a convenient matrix formulation for the transform pair. Let us consider a $2^n \times 2^n$ matrix $H_n$ whose $(i,j)$-th entry $h_{ij}$ satisfies $h_{ij} = (-1)^{x(i)^T x(j)}$, where $x(i)^T x(j)$ denotes the inner product of the binary expansions of $i$ and $j$. If $f = [f_0\, f_1 \dots f_{2^n-1}]^T$ and $\hat{f} = \left[\hat{f}_0\, \hat{f}_1 \dots \hat{f}_{2^n-1}\right]^T$, then, from the fact that $H_n^{-1} = 2^{-n} H_n$, we get

$$f = H_n \hat{f} \tag{4}$$

and

$$\hat{f} = \frac{1}{2^n} H_n f\,. \tag{5}$$

Note that the matrix $H_n$ is the Hadamard symmetric transform matrix and can be recursively defined as

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}. \tag{6}$$

We now present an interesting application of harmonic analysis to circuit complexity, due to Linial et al. [8].

As we have already mentioned, one of the best known results in circuit complexity is that $AC^0$ circuits require exponential size to compute the parity function. More precisely, $AC^0$-circuits cannot even approximate the parity function. This fact has a direct consequence on the Fourier transform, because, as we have already mentioned, the Fourier coefficients measure the correlation between the function and the parity of subsets of its input bits. Consequently, each high order Fourier coefficient of an $AC^0$ function must be very small (where "high order" means coefficients corresponding to strings of large cardinality). By exploiting this fact, Linial et al. were able to prove that not only is each individual high order coefficient small, but in fact the sum of squares (i.e. the *power spectrum*) associated with all high Fourier coefficients is very small.

**Lemma 1 (Spectral lemma [8])**
*Let $f$ be a Boolean function on $n$ variables computable by a Boolean circuit of depth $d$ and size $M$, and let $\theta$ be any integer. Then*

$$\sum_{|w|_1>\theta} (\hat{f}(w))^2 \leq \frac{1}{2} M 2^{-\frac{\theta^{1/d}}{20}} . \tag{7}$$

□

## 4 The Classes $\mathcal{B}_n^{(p)}$ and their Levels $B^{(p,k)}$.

In this section we define classes of functions which generalize the notion of *k-balanced functions* introduced in [1]. Let $p$ be a positive rational number, $0 < p \leq 1$.

**Definition 1 (Class $\mathcal{B}_n^{(p)}$)**
*$\mathcal{B}_n^{(p)}$ is the class of Boolean functions depending on $n$ variables that take the value 1 with probability $p$, i.e. on exactly $2^n p$ input strings.*

Making use of the notion of *restriction* (see Section 2), we organize the functions in each class $\mathcal{B}_n^{(p)}$ into a sequence of *levels*. Let $k$ be a positive integer such that $\log \frac{1}{p} \leq k \leq n$, and let us assume that $2^k p$ takes an integer value.

**Definition 2 ($k$-th level of $\mathcal{B}_n^{(p)}$)**
*$B^{(p,k)}$ is the subset of $\mathcal{B}_n^{(p)}$ consisting of all functions $f$ such that, for any restriction $\rho$ of size $k$, $f_\rho \in \mathcal{B}_k^{(p)}$. We call $B^{(p,k)}$ the $k$-th* level *of $\mathcal{B}_n^{(p)}$.*

In other words, $B^{(p,k)}$ consists of all functions $f$ which take the value 1 with probability $p$, such that any subfunction $f_\rho$ depending on $k$ variables, takes the value 1 again with probability $p$.

We now state some basic properties of the hierarchy of levels $B^{(p,k)}$. Let $k$ be a positive integer, such that $\log \frac{1}{p} \leq k \leq n$. Then.

- $B^{(p,k)} \subseteq B^{(p,k+1)}$.
- $B^{(p,n)} = \mathcal{B}_n^{(p)}$.
- The classes of $k$-balanced functions defined in [1] correspond to the $k$-th level of $\mathcal{B}_n^{(1/2)}$.
- The parity function and its complement are the only two functions which belong to the first level of $\mathcal{B}_n^{(1/2)}$, i.e. to $B^{(1/2,1)}$.

The first two properties follow immediately from the definition of the hierarchy; for the last two, we refer the reader to [1].

In Section 7 we will prove that, for any $p$, $B^{(p,k)}$ is *strictly* contained in $B^{(p,k+1)}$ and that the levels $B^{(p,k)}$ are not empty, provided that

$$k > \frac{\log p + 1}{\log p}\, n\,. \tag{8}$$

Notice that, in the special case $p = 1/2$, it turns out that

$$B^{(1/2,k)} \subset B^{(1/2,k+1)} \tag{9}$$

and that the levels $B^{(1/2,k)}$ are not empty, for any value of $k$, $1 \le k \le n$ (see [1] for more details).

All these proofs will make use of the spectral characterization of these functions, which we derive in the following section.

## 5 Spectral Characterization of the Hierarchy of $\mathcal{B}_n^{(p)}$ Functions

We now derive a spectral characterization of the functions in any level of the class $\mathcal{B}_n^{(p)}$. We denote by $\hat{f}_0$ the zero-order Fourier coefficient.

**Theorem 2 (Spectral characterization)**

*A Boolean function $f : \{0,1\}^n \to \{0,1\}$ belongs to the k-th level of the class $\mathcal{B}_n^{(p)}$ if and only if the following property holds:*

*(1)* $f \in \mathcal{B}_n^{(p)}$*;*

*(2) for any string w such that* $0 < |w|_1 \le n-k$, $\hat{f}(w) = 0$.

*Proof*

- We start by proving the "only if" side of the theorem. Let $f \in \mathcal{B}_n^{(p)}$ and $\mu \equiv (\mu_1, \mu_2, \ldots, \mu_n)$ be a Boolean string such that

  $$0 < |\mu|_1 = n - \ell \le n - k\,.$$

  Moreover, let

  $$U = \{i \mid \mu_i = 1\}\,.$$

  For any string $u \in \{0,1\}^{n-\ell}$, let $f_u$ denote the subfunction defined by the restriction that assigns to the variables $x_i$ such that $i \in U$, the $(n-\ell)$ values taken from the string $u$, and leaves undetermined the other $\ell$ variables.

  Then, we have

  $$\begin{aligned}
  \hat{f}(\mu) &= \frac{1}{2^n}\sum_w (-1)^{\mu^T w} f(w) = \frac{1}{2^n}\sum_w (-1)^{\sum_{i\in U} w_i} f(w) \\
  &= \frac{1}{2^n}\sum_{u\in\{0,1\}^{n-\ell}} \left[(-1)^{|u|_1} \sum_{v\in\{0,1\}^{\ell}} f_u(v)\right] \\
  &= \frac{1}{2^n}\sum_{u\in\{0,1\}^{n-\ell}} \left[(-1)^{|u|_1}\, |f_u|\right].
  \end{aligned}$$

For any $u \in \{0,1\}^{n-\ell}$, the subfunction $f_u$ depends on $\ell \geq k$ variables and, since $f \in B^{(p,k)}$, and $B^{(p,k)} \subseteq B^{(p,\ell)}$ for any $\ell \geq k$, we have $f_u \in \mathcal{B}_\ell^{(p)}$ and $|f_u| = 2^\ell p$. Thus, we get

$$\hat{f}(\mu) = \frac{2^\ell p}{2^n} \sum_{u \in \{0,1\}^{n-\ell}} (-1)^{|u|_1} = 0\,.$$

- We now prove the "if" side of the theorem, i.e., if properties (1) and (2) hold, then $f \in B^{(p,k)}$.

  Let us choose $(n-k)$ variables out of $n$, and let $U$ be the set of the indices of these $(n-k)$ variables. For any $u \in \{0,1\}^{n-k}$, let $f_u$ denote the subfunction obtained from $f$ by assigning to the variables in the set $U$, the $(n-k)$ values taken from the string $u$, and leaving undetermined the other $k$ variables.

  For any $u$, $f_u$ depends on $k$ variables. We show that any such subfunction takes the value 1 with probability $p$.

  Let $f_\#$ denote a vector whose entries are given by the cardinality of the $2^{n-k}$ subfunctions $f_u$, and let $\hat{f}_U$ denote a vector whose entries are the Fourier coefficients related to the $2^{n-k}$ strings $w \equiv (w_1, w_2, \ldots, w_n)$ such that $w_i = 0$ for any $i \notin U$. Note that all the $2^{n-k}$ coefficients in the vector $\hat{f}_U$ are of order less than or equal to $n-k$. Because of the recursive definition of Hadamard matrices, it turns out that

$$\hat{f}_U = \frac{1}{2^n}\, H_{n-k}\, f_\#\,.$$

  From property (2) and from the fact that the zero order Fourier coefficient is equal to the probability that the function takes the value 1, it then follows

$$\hat{f}_U = p \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

  from which

$$\begin{aligned} f_\# &= 2^n\, H_{n-k}^{-1}\, \hat{f}_U = \frac{2^n}{2^{n-k}}\, H_{n-k}\, \hat{f}_U \\ &= 2^k\, p\, H_{n-k} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 2^k\, p \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}. \end{aligned}$$

  Thus, the theorem follows by repeating the same argument for all the $\binom{n}{k}$ choices of the set $U$.

$\square$

# 6 A Lower Bound on the Size Complexity of $\mathcal{B}_n^{(p)}$ Functions

We are now able to prove our main result, i.e., that $AC^0$-circuits cannot compute functions in the $k$-th level of $\mathcal{B}_n^{(p)}$, whenever $k = n - (\log n)^{\omega(1)}$ and $p = \Omega(2^{-\mathrm{polylog}\, n})$.

We first make use of the spectral characterization derived in Theorem 2, together with Lemma 1, to determine a lower bound on the size required by a depth $d$ circuit to compute functions in the $k$-th level of $\mathcal{B}_n^{(p)}$. Finally, an easy application of this bound will provide our thesis.

In the following we will assume that $p \leq \frac{1}{2}$ (if $p > \frac{1}{2}$ we can consider the function $\neg f$ which has the same size complexity as $f$).

**Theorem 3 (Size complexity)**
*Let $f \in B^{(p,k)}$, $p \leq \frac{1}{2}$, be a Boolean function depending on n variables, computable by a circuit of constant depth $d$ and size $M$. Then*

$$M \geq 2^{\frac{(n-k)^{1/d}}{20}}\, p\,. \tag{10}$$

*Proof* An application of Lemma 1 yields the following inequality:

$$M \geq 2^{\frac{\theta^{1/d}}{20}}\, 2 \sum_{|w|_1 > \theta} (\hat{f}(w))^2\,.$$

Let us choose $\theta = n-k$. From the fact that $\hat{f}(w) = 0$ for any $0 < |w|_1 \leq n-k$ (see Theorem 2) it follows that

$$\sum_{|w|_1 > n-k} (\hat{f}(w))^2 = \sum_{w:|w|_1 \neq 0} (\hat{f}(w))^2 = \sum_{w} (\hat{f}(w))^2 - (\hat{f}_0)^2\,,$$

where $\hat{f}_0$ denotes the zero-order Fourier coefficient. Then, by using the *Parseval's identity*

$$\sum_{v} (\hat{f}(v))^2 = \hat{f}_0 = p\,,$$

we get

$$\sum_{|w|_1 > n-k} (\hat{f}(w))^2 = p - p^2 \geq \frac{p}{2}\,,$$

and the thesis immediately follows:

$$M \geq 2^{\frac{(n-k)^{1/d}}{20}}\, 2 \sum_{|w|_1 > n-k} (\hat{f}(w))^2 = 2^{\frac{(n-k)^{1/d}}{20}}\, p\,.$$

□

Notice how this result establishes a clear connection between complexity and combinatorial properties of Boolean functions.

Our main result, stating that $AC^0$-circuits cannot compute functions in the $k$-th level of $\mathcal{B}_n^{(p)}$, whenever

$$k = n - (\log n)^{\omega(1)}\,, \tag{11}$$

and

$$p = \Omega(2^{-\text{polylog}\, n})\,, \tag{12}$$

follows immediately as a corollary of Theorem 3.

**Corollary 4** *Any function* $f \in B^{(\Omega(2^{-polylog\, n}),\; n-(\log n)^{\omega(1)})}$ *requires superpolynomial size to be computed by a constant depth circuit.*

*Proof* Easily follows from Theorem 3. $\square$

Note how the lower bound to the size can become exponential:

**Corollary 5** *Constant depth circuits require exponential size to compute functions in levels* $B^{(p,k)}$ *whenever* $k$ *is s.t.* $n-k=\Omega(n^{\varepsilon})$*, for any positive constant* $\varepsilon<1$*, and* $p=\Omega(2^{-polylog\, n})$*.*

*Proof* Immediate from Theorem 3. $\square$

# 7 Properties of the Hierarchy $\mathcal{B}_n^{(p)}$

In this section we prove that nontrivial functions do exist in the levels of the hierarchy $\mathcal{B}_n^{(p)}$.

More precisely, we assume that $p=\frac{1}{2^t}$, where $t=t(n)$ is an integer, and, by applying the spectral characterization derived in Section 5, we prove that $B^{(p,k)}$ is strictly contained in $B^{(p,k+1)}$ and that the sets $B^{(p,k)}$ are not empty, provided that

$$k > \frac{\log p+1}{\log p}\, n\,, \tag{13}$$

i.e. $k>\frac{t-1}{t}\,n$.

Notice that, in the special case $p=1/2$, i.e. $t=1$, it turns out that

$$B^{(1/2,k)} \subset B^{(1/2,k+1)} \tag{14}$$

and that the levels $B^{(1/2,k)}$ are not empty, for any value of $k$, $1\le k\le n$ (see [1] for more details).

**Theorem 6**
*Let* $p=\frac{1}{2^t}$*. For any* $n$*,* $B^{(2^{-t},k)}\neq\emptyset$ *if* $k>\frac{t-1}{t}\,n$*.*

*Proof* By induction on $t$.

**Base**

For any $n$, and for $t=1$, the parity function and its complement belong to $B^{(1/2,1)}$ and $\frac{t-1}{t}\,n=0$.

**Induction step**

Let us suppose that, for any $n$, $B^{(2^{-t},k)}\neq\emptyset$ if $k>\frac{t-1}{t}\,n$.

Let $g$ be a Boolean function, depending on $n-1$ variables, which belongs to $B^{(2^{-t},k)}$ for $k=\frac{t-1}{t}\,(n-1)+1$ (to simplify the exposition, let us assume that $t$ divides $n-1$).

We define $f$, depending on $n$ variables, as follows:

$$f(\alpha\beta)=\begin{cases}0 & \text{if } \alpha=0\\ g(\beta) & \text{if } \alpha=1\,,\end{cases}$$

where $\alpha\in\{0,1\}$ and $\beta\in\{0,1\}^{n-1}$. First of all, note that $f\in\mathcal{B}_n^{2^{-(t+1)}}$. Indeed, $|f|=|g|=2^{n-(t+1)}$.

From the definition of $f$, and from the structure of Hadamard matrices, it turns out that the spectrum of $f$ can be defined in terms of the spectrum of $g$, in the following way:

$$\hat{f}(\alpha\beta) = \begin{cases} \frac{1}{2}\hat{g}(\beta) & \text{if} \quad \alpha = 0 \\ -\frac{1}{2}\hat{g}(\beta) & \text{if} \quad \alpha = 1\,. \end{cases}$$

If we now use the fact that $g \in B^{(2^{-t},\,\frac{t-1}{t}(n-1)+1)}$, together with the spectral characterization of Theorem 2, we obtain that $\hat{f}(w) = 0$, whenever $|w|_1 < \frac{n-1}{t}$. In particular, we have that $\hat{f}(w) = 0$ whenever $|w|_1 < \lfloor \frac{n}{t+1} \rfloor$, and from Theorem 2 it follows that $f \in B^{(2^{-(t+1)},k)}$ for $k > \frac{t}{t+1}n$, which completes our induction. $\square$

Notice that, because of its construction, the function $f$ defined in the proof of the above theorem is nondegenerated, i.e. it depends on all input variables.

By defining $f$ in a more complicated way it is possible, in some cases, to decrease the bound on $k$, but only by a constant factor. Therefore, we conjecture that the bound on $k$ given in Theorem 6 is not far from being asymptotically optimal.

Theorem 6 is an interesting result for the following two reasons. First of all, it allows us to verify that the classes of functions under investigation are not empty, at least for a significant number of levels. Moreover, since for constant values of the probability $p$, the functions in the deepest levels of the hierarchy can be regarded as "generalizations" of the parity function, it is interesting to understand how "deep" we can go in such a generalization, i.e. how close the combinatorial structure of level $k$ functions is to the combinatorial structure of parity.

We now prove that, for $p = 2^{-t}$, $B^{(2^{-t},k)}$ is strictly contained in $B^{(2^{-t},k+1)}$, provided that $k > \frac{t-1}{t}n$. In other words, we prove that nontrivial examples of functions do exist for those levels of $\mathcal{B}_n^{(2^{-t})}$ where $k > \frac{t-1}{t}n$.

**Theorem 7**
*Let $p = 2^{-t}$. If $k > \frac{t-1}{t}n$, then $B^{(2^{-t},k)}$ is strictly contained in $B^{(2^{-t},k+1)}$.*

*Proof* The proof of the theorem is easily derived from that of Theorem 6. For $t = 1$, $B^{(1/2,k)}$ is strictly contained in $B^{(1/2,k+1)}$ for any $k \geq 1$ (see [1]).

Let $g$ be a Boolean function, depending on $n-1$ variables, which belongs to $B^{(2^{-t},k)}$ but not to $B^{(2^{-t},k-1)}$, for $k = \frac{nt}{t+1} > \frac{t-1}{t}(n-1)$. Then, the induction step can easily be proved by considering a function $f$ defined as in the proof of Theorem 6. $\square$

# 8 Conclusion

Any attempt to find connections between mathematical properties and complexity has a strong relevance to the field of Complexity Theory. This is due to the lack of mathematical techniques to prove lower bounds for general models of computation. This work represents a step in this direction: we define a combinatorial property that makes Boolean functions "hard" to compute in constant depth and show how the Fourier transform could be used as a mathematical tool for the analysis of Boolean functions complexity. Further work to be done includes a deeper analysis of the structure of the levels $B^{(p,k)}$, in order to get an optimal lower bound on $k$, and, more in general, a deeper analysis of the connections between combinatorial properties, spectral properties and complexity of Boolean functions.

# References

[1] A. BERNASCONI. *On the complexity of balanced Boolean functions.* Information Processing Letters, Vol. **70**, pp. 157-163, 1999.

[2] A. BERNASCONI, C. DAMM, I. E. SHPARLINSKI. *Circuit and decision tree complexity of some number theoretic problems.* Information and Computation, to appear, 2000.

[3] A. BERNASCONI, I. E. SHPARLINSKI. *Circuit complexity of testing square-free numbers.* Proceedings of the 16th Ann. Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science **1563**, pp. 47-56, 1999.

[4] M. FURST, J. SAXE, M. SIPSER. *Parity, circuits, and the polynomial-time hierarchy.* Math. Syst. Theory, Vol. **17**, pp. 13-27, 1984.

[5] J. HÅSTAD. *Computational limitations for small depth circuits.* Ph.D. Dissertation, MIT Press, Cambridge, Mass., 1986.

[6] S.L. HURST, D.M. MILLER, J.C. MUZIO. *Spectral Method of Boolean Function Complexity.* Electronics Letters, Vol. **18 (33)**, pp. 572-574, 1982.

[7] R. J. LECHNER. *Harmonic Analysis of Switching Functions.* In *Recent Development in Switching Theory*, Academic Press, pp. 122-229, 1971.

[8] N. LINIAL, Y. MANSOUR, N. NISAN. *Constant Depth Circuits, Fourier Transform, and Learnability.* Journal of the ACM, Vol. **40 (3)**, pp. 607-620, 1993.

[9] H .U. SIMON. *A tight $\Omega(\log\log n)$ bound on the time for parallel RAM's to compute nondegenerate Boolean functions.* FCT'83, Lecture Notes in Computer Science **158**, 1983.

[10] I. WEGENER. *The complexity of Boolean functions.* Wiley-Teubner Series in Comp. Sci., New York – Stuttgart, 1987.

[11] A.C.-C. YAO. *Separating the polynomial-time hierarchy by oracles.* Proceedings of the 26th Ann. IEEE Symposium on Foundations of Computer Science, pp. 1-10, 1985.