International Journal of Foundations of Computer Science

A NOTE ON THE POLYNOMIAL REPRESENTATION OF BOOLEAN FUNCTIONS OVER $GF(2)$*

RICHARD BEIGEL†
Dept. of Electrical Engineering and Computer Science
University of Illinois at Chicago (M/C 154)
851 S Morgan St Fl 11
Chicago IL 60607-7053, USA

and

ANNA BERNASCONI‡
Lehrstuhl Effiziente Algorithmen
Institut für Informatik
Technische Universität München,
D-80290 München (Germany)

Received (received date)
Revised (revised date)
Communicated by Editor's name

ABSTRACT

We investigate the representation of Boolean functions as polynomials over the field $GF(2)$, and prove an interesting characterization theorem: the degree of a Boolean function over $GF(2)$ is equal to the size of its largest subfunction that takes the value 1 on an odd number of input strings. We then present some properties of *odd* functions, i.e., functions that take the value 1 on an odd number of strings, and analyze the connections between the problem of the existence of odd functions with very low maximal sensitivity and the long standing open problem of the relationship between the maximal sensitivity and the block sensitivity of Boolean functions.

1. Introduction

Over the last decade, several authors have employed polynomial methods in circuit complexity [2]. A key step in this approach is showing that Boolean functions computable by certain kinds of circuits can be represented by polynomials of a given type, e.g., low-degree polynomials.

Every Boolean function can be represented as a polynomial. Let f be a Boolean function on n variables and $p : F^n \to F$ a multivariate polynomial over a field F.

*A preliminary version of this paper was published in *Proceedings of the 6th Italian Conference On Theoretical Computer Science* (ICTCS'98), pp. 265–276, World Scientific 1998.

†`beigel@uic.edu`, `http://learn.at/theory/beigel`. Also with DIMACS. Supported in part by NSF grants CCR-9996021, CCR-9877150, and CCR-???.

‡`bernasco@informatik.tu-muenchen.de`

We say that p *represents* f if, for every $w \in \{0,1\}^n$, $f(w) = p(w)$. Since $x^2 = x$ for all variables $x \in \{0,1\}$, the polynomials are automatically multilinear.

In this note we focus our attention on the representation of Boolean functions by polynomials over the field $GF(2)$, and prove that the degree of a Boolean function over $GF(2)$ is equal to the size of its largest subfunction that takes the value 1 on an odd number of input strings. We then discuss some peculiar properties of *odd* functions, i.e., functions that take the value 1 on an odd number of strings, and analyze the connections between the problem of the existence of odd functions with very low maximal sensitivity and the long standing open problem of the relationship between the maximal sensitivity and the block sensitivity of Boolean functions (see [3, 5, 7]).

1.1. Preliminaries

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; and the *set notation*, based on the correspondence between the set $\{0,1\}^n$ and the power set of $\{1,2,\ldots,n\}$.

Given a string $w \in \{0,1\}^n$, we denote with $w^{(i)}$ the string obtained from w by flipping its i-th bit $(1 \leq i \leq n)$, i.e., w and $w^{(i)}$ differ only on the i-th bit. Moreover, given a subset of indices $B \subseteq \{1,2,\ldots,n\}$, we denote by $w^{(B)}$ the string w with all bits in B flipped, i.e., $w^{(B)}$ differs from w exactly on B.

We will denote with $|f|$ the number of strings accepted by the function f, i.e., $|f| = |\{w \in \{0,1\}^n : \ f(w) = 1\}|$. The notation $|w|$ denotes the *Hamming weight* of the string w, i.e., number of ones in it. Finally, all the logarithms are to the base 2.

We now review the notion of *restriction.*

Definition 1 *A* restriction ρ *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.*

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

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

2. Some Measures of Complexity for Boolean Functions

In this section we briefly review some results concerning the relationships between several complexity measures for Boolean functions.

Sensitivity. The *sensitivity* of a Boolean function is a measure of how the value of the function is sensitive to changes in the input. Let f be a Boolean function depending on n binary variables. The *sensitivity* of f on the string $w \in \{0,1\}^n$, $s_f(w)$, is the number of locations i for which $f(w) \neq f(w^{(i)})$, i.e.,

$$s_f(w) = \sum_{i=1}^{n} (f(w) - f(w^{(i)}))^2 \,.$$

The *average sensitivity* of f, $s(f)$, is the average of $s_f(w)$ over all $w \in \{0,1\}^n$, taken with respect to the uniform distribution:

$$s(f) = \frac{1}{2^n} \sum_{w} s_f(w) = \mathbf{E}[s_f(w)] \,.$$

The *maximal sensitivity* of f is defined as

$$S_{max}(f) = \max_{w} \{s_f(w)\} \,.$$

This measure has been discussed in the literature under various names, e.g., it is sometimes called 'critical complexity' [12].

Block sensitivity. The notion of *block sensitivity*, denoted $BS(f)$, has been introduced by Nisan in [6], who used it to obtain a full characterization of the time needed to compute a Boolean function on a CREW PRAM with an unlimited number of processors. The block sensitivity is an extension of the maximal sensitivity, in which we are allowed to invert a block of bits simultaneously. Let $B \subseteq \{1,2,\ldots,n\}$ be a subset of indices and let w be a Boolean string of length n. We say that the function f is sensitive to the subset $B \subseteq \{1,2,\ldots,n\}$ on w if $f(w) \neq f(w^{(B)})$. The *block sensitivity* of f on w, $BS_f(w)$, is the largest number t such that there exists t *disjoint* sets $B_1, B_2, \ldots, B_t$ such that, for all $1 \leq i \leq t$, f is sensitive to B_i on w. The *block sensitivity* of f, $BS(f)$, is the maximum over all w of the block sensitivity of f on w. It is obvious that for any function f, $S_{max}(f) \leq BS(f)$, since the sensitivity is just the block sensitivity with all blocks of length one.

Deterministic decision tree complexity. The *deterministic decision tree complexity* of a function f, denoted $D(f)$, is given by the minimal depth of a Boolean decision tree for n variables that computes f. Note that $D(f)$ is nothing but the number of bits read on the worst case input by the best deterministic algorithm in order to determine the value of the function f.

Certificate complexity. A 1-*certificate* (0-*certificate*) for f is an assignment to some subset of the variables that forces the value of f to 1 (0). The *certificate complexity of f on w*, denoted $c_f(w)$, is the size of the smallest certificate that agrees with w. The *certificate complexity of* f, denoted $C(f)$, is the maximum, over all w, of $c_f(w)$. The certificate complexity of a function describes how many bits of the input must be revealed to you (by someone who knows all the input bits) in order to convince you of the value of the function.

We now mention the known relationships between these complexity measures.

Lemma 1 ([6]) *For any function f, $S_{max}(f) \leq BS(f) \leq C(f)$.*

It turns out that for a large subclass of functions these three measures of complexity are actually equal:

Lemma 2 ([6]) *For any monotone function f, $S_{max}(f) = BS(f) = C(f)$.*

Notice that for general, nonmonotone functions the inequalities can be strict. For instance, the symmetric function

$$f(w) = \begin{cases} 1 & \text{if } |w| = \frac{n}{2}, \frac{n}{2}+1, \\ 0 & \text{otherwise}, \end{cases}$$

has maximal sensitivity $\frac{n}{2}+1$, block sensitivity $\frac{3}{4}n$, and certificate complexity $n-1$ (for simplicity, assume that 4 divides n).

In the general case the relationships between maximal and block sensitivity are not clear. All we know is that $BS(f)$ and $S_{max}(f)$ are polynomially related when $BS(f) = \Omega(n)$ [5]. Moreover, Rubinstein [8] exhibited an infinite family G of functions with a quadratic gap between the sensitivity and the block sensitivity, and in [3] it was shown that in the *average case* there is no polynomial (or even exponential) relationship between sensitivity and block sensitivity. In the maximal case it is still an open problem whether the gap between the two measures may be super-polynomial.

With respect to the relationship between block sensitivity and certificate complexity, Nisan proved that these two measures are polynomially related.

Lemma 3 ([6]) *For all Boolean functions f, $C(f) \leq BS^2(f)$.*

We conclude this section by mentioning the relationships between the decision tree complexity, the certificate complexity and the block sensitivity.

Lemma 4 ([1]) *For all Boolean functions f, $C(f) \leq D(f) \leq C(f)\,BS(f)$.*

3. Polynomial Representation of Boolean Functions

Boolean functions may be represented in various forms. Some of the simplest and most natural of these forms are representations as polynomials over various fields. Since $x^2 = x$ for all variables $x \in \{0,1\}$, these polynomials are automatically multilinear.

Definition 2 *Let f be a Boolean function on n variables and $p : \mathsf{R}^n \to \mathsf{R}$ a multivariate polynomial over the reals. We say that p* represents *f if, for every $w \in \{0,1\}^n$, $f(w) = p(w)$.*

The polynomial representation of a function over $GF(2)$ can be obtained from its real polynomial representation, by simply keeping those monomials with an odd coefficient and by giving them the value 1 as new coefficient. Indeed, we have the following proposition:

Proposition 1 ([10]) *The polynomial representation of Boolean functions over the field $GF(2)$ is given by the polynomial in the real case, except the coefficients are taken modulo 2.*

The basic parameter of the representation of a Boolean function as a polynomial is its *degree*.

Definition 3 *For a Boolean function f, the* degree *of f over a field F, denoted by $d_F(f)$, is the degree of the unique multilinear polynomial over F that represents f.*

With $d_R(f)$ and $d_2(f)$ we will then denote the degree of a function f over R and over $GF(2)$, respectively. Obviously, $d_2(f) \leq d_R(f)$.

The degree of a function over the reals can be related to several complexity measures. For instance, for any Boolean function f, we have $d_R(f) \leq D(f)$ and $d_R(f) \geq \sqrt{BS(f)}$ (see [10, 7] for more details). With respect to the degree of a function over Z_m, some interesting lower bound can be found in [11].

4. Characterization of the Degree of a Function over $GF(2)$

We now provide an interesting characterization of the degree of a Boolean function over $GF(2)$. More precisely, given a function f, we prove that $d_2(f)$ is equal to the size of the largest subfunction of f that takes the value 1 on an odd number of input strings.

To this aim, we first introduce the following definition:

Definition 4 *A Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is* odd *if $|f|$ is an odd number,* even *if $|f|$ is an even number.*

We now state a lemma that the reader may easily prove from first principles.

Lemma 5 *Let g be a Boolean function. If g depends on more than $d_2(g)$ variables, then g is an even function.*

Theorem 1 *Let f be a Boolean function depending on n variables. Then, $d_2(f)$ is equal to the size of the largest odd subfunction of f.*

Proof. Let g be any subfunction of f. Then $d_2(g) \leq d_2(f)$. If g depends on more than $d_2(f)$ variables, then g is even by Lemma 5. Thus the size of the largest odd subfunction of f is less than or equal to $d_2(f)$.

To show that this inequality is tight, consider a monomial $x_{i_1}x_{i_2}\cdots x_{i_d}$ of degree $d = d_2(f)$ in the polynomial representation of f over $GF(2)$, and let g denote the restriction of f to the set of variables $\{x_{i_1}, x_{i_2}, \ldots, x_{i_d}\}$. By Lemma 5, $g - x_{i_1}x_{i_2}\cdots x_{i_d}$ is even. Since $x_{i_1}x_{i_2}\cdots x_{i_d}$ is odd, g is odd. □

Corollary 1 *A Boolean function f on n variables is odd if and only if $d_2(f) = n$.*

5. Odd Functions and the Sensitivity vs. Block Sensitivity Problem

In this section we restrict our attention to the class of odd functions, and analyze the connections between the problem of the existence of odd functions with very low maximal sensitivity and that of the relationships between maximal and block sensitivity of Boolean functions. We then conclude with an observation regarding the class of *read-once functions.*

The following proposition is an easy consequence of Theorem 1 and of the results reviewed in Section 2.

Proposition 2 *For any odd function f, $D(f) = n$, $C(f) \geq \sqrt{n}$, and $BS(f) \geq \sqrt[3]{n}$.*

The lower bound on the certificate complexity of odd functions is tight and it is achieved, e.g., by the following odd function (for simplicity, assume that n is a perfect square):

$$h = \bigwedge_{i=1}^{\sqrt{n}} g_i \quad \text{with} \quad g_i = \bigvee_{j=1}^{\sqrt{n}} x_{i_j} . \tag{1}$$

Since for monotone functions we have $S_{max}(f) = BS(f) = C(f)$, from Proposition 2 it follows that odd monotone functions must have high maximal sensitivity: $S_{max}(f) \geq \sqrt{n}$. Note that this bound is tight and it is again reached by the odd monotone function (1). On the contrary, there exist even monotone functions with very low maximal sensitivity, e.g., the *monotone address function*, which has maximal sensitivity $O(\log n)$ [12].

We now analyze the connections between the problem of the existence of odd functions with very low maximal sensitivity and that of the relationships between the maximal sensitivity and the block sensitivity of Boolean functions. First, we observe how the existence of an odd function with polylogarithmic maximal sensitivity would imply the existence of an exponential gap between the maximal and the block sensitivity, as a consequence of the fact that for any odd function f, $BS(f) \geq \sqrt[3]{n}$.

Proposition 3 *Let $f : \{0,1\}^n \to \{0,1\}$ be an odd Boolean function. If $S_{max}(f) = (\log n)^{O(1)}$, then f presents an exponential gap between its maximal sensitivity and its block sensitivity.*

Note that the existence of an odd function with a superpolynomial gap between maximal and block sensitivity implies the existence of an even function with the same property. In fact, if $f : \{0,1\}^n \to \{0,1\}$ has this property, then by concatenating f and its complement $\neg f$, we get a nondegenerate even function $h : \{0,1\}^{n+1} \to \{0,1\}$, such that $S_{max}(h) = S_{max}(f) + 1$ and $BS(h) = BS(f) + 1$.

Proposition 3 suggests how the problem of finding a nontrivial lower bound on the maximal sensitivity of odd functions should be quite difficult. In fact, by exhibiting an odd function with polylogarithmic maximal sensitivity, we will immediately solve the long-standing open problem of the relationship between maximal and block sensitivity (see [3, 5, 7]). Anyway, it would be interesting to understand in a deeper way the connections between these two problems. To this aim, we define the following subclass of even Boolean functions:

Definition 5 *Let f be a Boolean function depending on n variables. We say that f is* strongly-even *if its degree over $GF(2)$ is a constant independent of n.*

We now prove that strongly-even Boolean functions cannot present a superpolynomial gap between maximal and block sensitivity. We will use a result proved in [5].

Definition 6 *Given an integer ℓ, the ℓ-*block sensitivity *of a function f on a string w is defined to be the largest number t such that there exists t* disjoint *sets $B_1, B_2, \ldots, B_t$ such that, for any $1 \leq i \leq t$,*

- $|B_i| \leq \ell$;
- *f is sensitive to B_i on w.*

*The ℓ-*block sensitivity *of f, $BS_\ell(f)$, is the maximum, over all w, of the ℓ-block sensitivity of f on w.*

Theorem 2 ([5]) *For any Boolean function f, $BS_\ell(f) = O\left((S_{max}(f))^\ell\right)$.*

Lemma 6 *For any strongly-even function f, $BS(f) = O\left((S_{max}(f))^{d_2(f)}\right)$.*

Proof. First observe that for any strongly-even function f we have $BS(f) = BS_\ell(f)$, where $\ell = d_2(f)$. This means that a strongly-even function can be sensitive only to blocks of constant (minimal) size. To see why this fact holds, let us consider any minimal-size block B such that f is sensitive to B on a string $w = (w_1, w_2, \ldots, w_n)$. The following two conditions hold

- $f(w) \neq f(w^{(B)})$;
- for any $C \subset B$, $f(w) = f(w^{(C)})$.

Now, observe that these conditions imply that the subfunction f_β, where β is the following restriction

$$\beta(x_i) = \begin{cases} w_i & \text{if } i \notin B \\ \star & \text{if } i \in B\,, \end{cases}$$

is an odd function. More precisely, it turns out that $|f_\beta| = 1$. From the characterization of $d_2(f)$ (see Theorem 1) it then follows that $|B| \leq d_2(f)$. □

Lemma 6 could be considered a weak support to the conjecture that among the class of even functions, only the functions of high degree over $GF(2)$ could present a superpolynomial gap between maximal and block sensitivity. Clearly, to settle this conjecture, we should be able to understand what happens to the block sensitivity of even functions whose degree over $GF(2)$ is of order $o(n)$. Unfortunately, at the moment this question seems to be as difficult as the 'sensitivity versus block sensitivity' problem.

We conclude this section with a remark regarding the class of *read-once* Boolean functions, i.e., functions computable by read-once formulas.

Remark 1 *Nondegenerate read-once Boolean functions have always maximum degree over $GF(2)$, i.e., they are odd functions.*

(The proof of this result, already pointed out in [9], is left to the reader.)

Since read-once functions can be regarded as monotone functions, from Proposition 2 it then follows that for any read-once function f depending on n variables $S_{max}(f) = BS(f) = C(f) \geq \sqrt{n}$. This lower bound is tight and it is again reached by the function (1).

6. Conclusion

In this note we have presented some results concerning the connections between combinatorial properties of Boolean functions and their complexity. Many of these are known results, and some are new. We have also noticed an interesting connection between two different 'combinatorial' problems: that of finding a lower bound on the maximal sensitivity of odd Boolean functions, and that of understanding the relationships between the sensitivity and the block sensitivity. We hope that this combinatorial approach could be further exploited to study the complexity of Boolean functions, and that our results could represent the starting point of a deeper analysis, that will eventually lead to the solution of the open problem concerning the interplay between maximal and block sensitivity.

Further work to be done includes a characterization of the degree of Boolean functions over Z_m, together with an analysis of the conjecture that among the class of even functions, only the functions of high degree over $GF(2)$ could present a large gap between maximal and block sensitivity.

7. References

1. R. Beals, H. Buhrman, R. Cleve, M. Mosca and R. de Wolf, "Quantum Lower Bounds by Polynomials," in *Proc. 39th FOCS*, 1998, pp. 352–361.
2. R. Beigel, "The Polynomial Method in Circuit Complexity," in *Proc. 8th Conf. Structure in Complexity Theory*, 1993, pp. 82–95.
3. A. Bernasconi, "Sensitivity vs. Block Sensitivity (an average-case study)," in *Information Processing Letters* **59**(3), 1996, pp. 151–157.
4. A. Bernasconi, "Mathematical Techniques for the Analysis of Boolean Functions," Ph.D. Thesis, University of Pisa, 1997.
5. C. Kenyon, "Sensitivity vs. Block Sensitivity of Boolean Functions," *DIMACS Technical Report* 90–18, 1990.
6. N. Nisan, "CREW PRAMs and Decision Trees," in *SIAM Journal on Computing* **20**(6), 1991, pp. 999–1007.
7. N. Nisan and M. Szegedy, "On the Degree of Boolean Functions as Real Polynomials," in *Proc. 24th STOC*, 1992, pp. 462–467.
8. D. Rubinstein, "Sensitivity vs. Block Sensitivity of Boolean Functions," in *Combinatorica* **15**, 1995.
9. M. Sitharam, "Evaluating Spectral Norms for Constant Depth Circuits with Symmetric Gates," in *Computational Complexity* **5**, 1995, pp. 167–189.
10. M. Szegedy, "Algebraic methods in lower bounds for computational models with limited communication," Ph.D. Thesis, University of Chicago, 1989.
11. S. C. Tsai, "Lower bounds on representing Boolean functions as polynomials in Z_m," in *Proc. 8th Conf. Structure in Complexity Theory*, 1993, pp. 96–101.
12. I. Wegener, *The complexity of Boolean functions* (Wiley–Teubner Series in Computer Science, New York–Stuttgart, 1987).