Diameter Versus Certificate Complexity of Boolean Functions

Siddhesh Chaubal
University of Texas at Austin, TX, USA

Anna Gál
University of Texas at Austin, TX, USA

Abstract

In this paper, we introduce a measure of Boolean functions we call *diameter*, that captures the relationship between certificate complexity and several other measures of Boolean functions. Our measure can be viewed as a variation on alternating number, but while alternating number can be exponentially larger than certificate complexity, we show that diameter is always upper bounded by certificate complexity. We argue that estimating diameter may help to get improved bounds on certificate complexity in terms of sensitivity, and other measures.

Previous results due to Lin and Zhang [20] imply that $s(f) \geq \Omega(n^{1/3})$ for transitive functions with constant alternating number. We improve and extend this bound and prove that $s(f) \geq \sqrt{n}$ for transitive functions with constant alternating number, as well as for transitive functions with constant diameter. We also show that $bs(f) \geq \Omega(n^{3/7})$ for transitive functions under the weaker condition that the "minimum" diameter is constant.

Furthermore, we prove that the log-rank conjecture holds for functions of the form $f(x \oplus y)$ for functions f with diameter bounded above by a polynomial of the logarithm of the Fourier sparsity of the function f.

2012 ACM Subject Classification Theory of computation → Complexity classes

Keywords and phrases Sensitivity Conjecture, Boolean Functions, Certificate Complexity, Block Sensitivity, Log-rank Conjecture, Alternating Number

Digital Object Identifier 10.4230/LIPIcs.MFCS.2021.31

Acknowledgements We thank the anonymous referees for helpful comments on a previous version of the paper.

1 Introduction

The alternating number of a Boolean function f, denoted $alt(f)$, measures how close the function is to being monotone. It was first studied by Markov [22], who showed that the minimum number of negation gates to compute f by any Boolean circuit is exactly $\lceil \log_2(alt(f) + 1) \rceil$. This led to further studies of alternating number in connection to understanding the effect of negation gates in various contexts such as circuit complexity [31, 34, 26, 27], learning theory [8], and cryptography [16].

Our work is motivated by an interesting paper of Lin and Zhang [20], who studied functions with small alternating number in the context of the sensitivity conjecture, and the log-rank conjecture for XOR functions. The sensitivity conjecture of Nisan and Szegedy [28] states that several important complexity measures, for example block sensitivity $bs(f)$, certificate complexity $C(f)$, and degree $deg(f)$ (over the reals) are all upper bounded by a polynomial of sensitivity $s(f)$. The sensitivity conjecture has been recently proved by Huang [17], who showed that for any Boolean function f, $deg(f) \leq s(f)^2$. Huang's result was further strengthened by Laplante et al. [19] and Aaronson et al. [1]. Both conjectures have been open for several decades, and – until Huang's result resolving the sensitivity conjecture – were verified only for a few special classes of Boolean functions. The log-rank conjecture is still open even for XOR functions.

Both conjectures can be easily verified to hold for monotone Boolean functions. Lin and Zhang [20] showed that both conjectures remain true for functions that are close to monotone, that is for functions with small alternating number. More precisely, they showed that the conjectures hold for functions with constant alternating number, as well as for functions with alternating number bounded above by some relevant complexity measures of the functions, such as sensitivity in the case of the sensitivity conjecture, and Fourier sparsity in the case of the log-rank conjecture for XOR functions. Thus, their work extended the class of functions where the conjectures can be verified. On the other hand, Dinesh and Sarma [14] presented a function f such that $alt(f)$ is exponentially larger than the certificate complexity $C(f)$. This means that the sensitivity conjecture and the log-rank conjecture for XOR functions cannot be proved in the general case by providing upper bounds on alternating number.

Diameter of Boolean functions. In this paper, we introduce a measure of Boolean functions we call *diameter*, that captures the relationship between certificate complexity and several other measures of Boolean functions. To define the diameter of a Boolean function f, we first consider the "distance" between a vertex of the Boolean cube and subcubes where the function f is constant. However, instead of measuring distance by the number of edges of the Boolean cube along a path (which would correspond to Hamming distance), we allow flipping several bits in one step. We consider paths in the Boolean cube, where one step of the path involves flipping a block of input bits of the function, thus each step specifies a subcube. We require that each step along a path corresponds to a subcube, where the subfunction of f satisfies certain conditions. We define several variants, by considering different classes of Boolean functions that can appear as subfunctions on the subcubes associated with the steps of a path.

For example, in the first variant of our measure, the requirement is that each step along the path corresponds to flipping bits of a minimal sensitive block of the function f. That is, for a step $x^{(i)}, x^{(i+1)}$ along such a path, the requirement is that $f(x^{(i)}) \neq f(x^{(i+1)})$, but $f(x^{(i)}) = f(y)$ for every $y \neq x^{(i+1)}$ from the subcube defined by the bits where $x^{(i)}$ and $x^{(i+1)}$ differ. Notice that this condition means that the subfunction of f restricted to the subcube associated with each step is either the AND function (when $f(x^{(i)}) = 0$) or the NAND function (when $f(x^{(i)}) = 1$). Generalizing this idea, we define several variants of our measure by specifying the class $\mathcal{H}$ of functions that can appear as subfunctions along the steps of a legal path.

Once we specified which steps are legal along a path for a given variant of our measure, we proceed as follows. For a given input x, we define the diameter of f on x as the length of the shortest "legal" path from $\bar{x}$ (the complement of x) to any certificate of f on x, that is to any constant subcube containing x. Then, similarly to standard complexity measures like certificate complexity, we take the maximum over all inputs. Depending on the class $\mathcal{H}$ of functions we allow to appear as subfunctions along the steps of a path, we obtain variants of our measure.

Comparison of diameter with alternating number. Our measure is motivated by alternating number, but it is quite different from it.

First, the similarity is that both measures involve considering paths in the Boolean cube, where one step of the path involves flipping a block of input bits of the function, thus each step specifies a subcube. For alternating number, the requirement on the function values on the subcubes is that the function takes different values on the two opposite (all 0 and all 1) points of the subcubes. For our measure, we consider different classes of Boolean functions that can appear as subfunctions on the subcubes associated with a path.

We note that the definition of alternating number also requires that a path is monotone, (that is the set of 1 bits of an input x on the path must be a subset of the 1 bits of any input that appears later in the path). We do not impose such requirement. In contrast to alternating number, diameter does not measure closeness to monotonicity.

Furthermore, alternating number considers the longest "legal" path between just two specific points, the all 0 input and the all 1 input. For our measure, we consider the shortest "legal" path between inputs x and subcubes corresponding to certificates of the function on the complementary input $\bar{x}$.

We note that in general, diameter and alternating number are incomparable, and we provide examples that illustrate this. However, an important distinction is that while alternating number can be exponentially larger than certificate complexity [14], each variant of our measure considered in this paper is upper bounded by certificate complexity, up to constant factors.

Diameter vs certificate complexity. We define the following variants, depending on the class $\mathcal{H}$ of functions we allow to appear as subfunctions along the steps of a path: $dia_\wedge$ where $\mathcal{H}$ consists of the functions AND and NAND (these are the possible subfunctions associated with minimal sensitive blocks, as discussed above), dia_s where $\mathcal{H}$ includes all functions with full sensitivity, dia_{deg} where $\mathcal{H}$ includes all functions with full real degree, dia_{deg_2} where $\mathcal{H}$ includes all functions with full $\mathbb{F}_2$-degree.

Note that each of the classes we consider contains the functions AND and NAND since both of these functions have full sensitivity, full $\mathbb{F}_2$-degree and full real degree. Thus, each of the measures $dia_s(f)$, $dia_{deg}(f)$ and $dia_{deg_2}(f)$ is upper bounded by $dia_\wedge(f)$, for every Boolean function f. On the other hand, as we illustrate by examples, $dia_s(f)$, $dia_{deg}(f)$ and $dia_{deg_2}(f)$ may be significantly smaller than $dia_\wedge(f)$, thus considering these variants may lead to stronger bounds. Furthermore, since $deg_2(f) \leq deg(f)$, we have that $dia_{deg}(f) \leq dia_{deg_2}(f)$. We also present examples showing that $dia_{deg}(f)$ may be significantly smaller than $dia_{deg_2}(f)$.

We prove that for all the classes $\mathcal{H}$ considered in this paper,

$$dia_{\mathcal{H}}(f) \leq dia_\wedge(f) \leq 2C(f).$$

Depending on the class $\mathcal{H}$, we can lower bound $dia_{\mathcal{H}}$ by certificate complexity divided by specific complexity measures, such as sensitivity. We show that for any Boolean function f, $C(f)/s(f)$ is upper bounded by $dia_s(f)$ and thus we can upper bound certificate complexity as follows:

$$C(f) \leq dia_s(f)s(f) \leq dia_\wedge(f)s(f).$$

Similarly, considering the classes $\mathcal{H}$ consisting of Boolean functions with full real degree and full $\mathbb{F}_2$-degree, respectively, we get the following bounds relating diameter and certificate complexity. For any Boolean function f, $C(f) \leq dia_{deg}(f)deg(f) \leq dia_\wedge(f)deg(f)$ and $C(f) \leq dia_{deg_2}(f)deg_2(f) \leq dia_\wedge(f)deg_2(f)$.

Other variants. One could consider more versions of our measure, for various other classes $\mathcal{H}$. Another class that is natural to consider in connection to the log-rank conjecture for XOR functions is taking $\mathcal{H}$ to be the class of Boolean functions with full Fourier sparsity, that is functions such that all their Fourier coefficients are nonzero. We do not discuss this variant in more details, as the results are analogous to our results on dia_{deg_2} with similar applications.

We would like to mention another version of our definitions, that turns out to be helpful in proving some of our results for special classes of Boolean functions. Several papers in the literature consider minimum certificate complexity, defined as $C_{min}(f) = min_x C(f,x)$. Similarly, while we define diameter as $dia_{\mathcal{H}}(f) = max_x dia_{\mathcal{H}}(f,x)$, we also consider minimum diameter defined as $dia_{min,\mathcal{H}}(f) = min_x dia_{\mathcal{H}}(f,x)$.

Results on transitive functions with small diameter. There has been a long line of work trying to estimate the sensitivity and block sensitivity for transitive functions [32] and also for special classes of transitive functions such as symmetric functions and graph properties [38, 33], minterm transitive functions and cyclically invariant functions [10, 2, 15], transitive functions with sparse DNFs [12].

It has been conjectured that all transitive functions must have "large" sensitivity and block sensitivity. No examples of transitive functions are known on n input bits with $o(n^{1/3})$ sensitivity. Chakraborty [10] constructed a transitive function on n variables with sensitivity $\Theta(n^{1/3})$. It is noted in [12] that an argument in [32] together with Huang's result gives that any transitive function f on n variables has $s(f) \geq \Omega(n^{1/6})$.

Previous results due to Lin and Zhang [20] imply that $s(f) \geq \Omega(n^{1/3})$ for transitive functions with constant alternating number. We improve and extend this bound and prove that $s(f) \geq \sqrt{n}$ for transitive functions with constant alternating number, as well as for transitive functions with constant diameter, considering dia_s or $dia_\wedge$.

Regarding block sensitivity, it has been conjectured that $\Omega(n^{3/7})$ is a lower bound on the block sensitivity of all transitive functions. There is an example of a transitive function f due to Amano [2] that has $bs(f) = \theta(n^{3/7})$, and no transitive function is known with smaller block sensitivity. Sun[32] proved a lower bound of $n^{1/3}$ on the block sensitivity for all transitive functions. Since block sensitivity is at least sensitivity, our result above also implies that for transitive functions with constant alternating number or constant diameter (dia_s or $dia_\wedge$), $bs(f) \geq \Omega(\sqrt{n})$. We prove that the conjectured $\Omega(n^{3/7})$ lower bound holds under a weaker condition, for all transitive functions with constant *minimum* diameter ($dia_{min,s}$ or $dia_{min,\wedge}$).

Log-rank conjecture for XOR functions with small diameter. The log-rank conjecture for functions of the form $f(x \oplus y)$ has been proved when f belongs to certain special classes such as monotone or linear threshold functions [25], symmetric functions [39], functions with low $\mathbb{F}_2$-degree or small spectral norm [35], AC^0 functions [18], read-k functions [11], and functions with constant alternating number by Lin and Zhang [20]. We prove that the log-rank conjecture holds for functions of the form $f(x \oplus y)$ for functions f with dia_{deg_2} or $dia_\wedge$ bounded above by a polynomial of the logarithm of the Fourier sparsity of f.

Further motivation for considering diameter. As we noted above, $dia_{\mathcal{H}}(f) \leq 2C(f)$ for any f and any class $\mathcal{H}$ that contains the functions AND and NAND. Huang's result implies that $C(f) = O(s(f)^5)$, which in turn implies that for any f, and any class $\mathcal{H}$ that contains the functions AND and NAND, (which means for every class considered in this paper), we have

$$dia_{\mathcal{H}}(f) = O(s(f)^5).$$

Obtaining new upper bounds on $dia_{\mathcal{H}}$ could lead to the following interesting consequences:

- An independent proof of the upper bound $dia_{\mathcal{H}}(f) \leq poly(s(f))$ for dia_s or $dia_\wedge$ could lead to an independent, purely combinatorial proof of the sensitivity conjecture.

- Improving the upper bound on dia_s or $dia_\wedge$ in terms of sensitivity to $dia_{\mathcal{H}}(f) \leq O(s(f)^2)$, would improve the current best upper bounds on block sensitivity and certificate complexity to $bs(f) \leq C(f) \leq O(s(f)^3)$.
  In connection to this question, we note that there are Boolean functions with $dia_s(f)$ (and thus $dia_\wedge(f)$) at least $\Omega(s(f)^{(2-o(1))})$, since [3] exhibited a function with $C(f) = \Omega(s(f)^{(3-o(1))})$ improving previous results of [6] and [5].
- Proving that $dia_{deg}(f) \leq deg(f)$ would imply the bound $C(f) \leq O(s(f)^4)$, using Huang's result, but improving its current implication which gives only $C(f) \leq O(s(f)^5)$. It would also imply that $C(f) \leq O(deg(f)^2)$, improving the current best bound giving $C(f) \leq deg(f)^3$ by [24].
  We note that there are Boolean functions with $dia_{deg}(f)$ (and thus $dia_{deg_2}(f)$ and $dia_\wedge(f)$) at least $\Omega(deg(f)^{(1-o(1))})$, since there are Boolean functions with $C(f) = \Omega(deg(f)^{(2-o(1))})$ which was shown recently in [3] improving the previous $\Omega(deg(f)^{1.63})$ bound of [29].
- Upper bounds on $dia_{\mathcal{H}}$ (considering an appropriate $\mathcal{H}$) for specific classes of Boolean functions could give stronger upper bounds on block sensitivity or certificate complexity in terms of sensitivity than currently known for these classes, and could verify the log-rank conjecture for XOR functions for new classes.

2 Preliminaries

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function and $x \in \{0,1\}^n$ be any input. For $i \in [n]$ we denote by x^i the input obtained by flipping the i-th bit of x. More generally, for $S \subseteq [n]$ we denote by x^S the input obtained by flipping the bits of x in all coordinates in the subset S.

For any two inputs $x, y \in \{0,1\}^n$, we say $x \prec y$ if $x_i \leq y_i$ for all $i \in [n]$.

▶ **Definition 2.1** (Sensitivity). *The sensitivity $s(f,x)$ of a Boolean function f on input x is the number of coordinates $i \in [n]$ such that $f(x) \neq f(x^i)$. The sensitivity of f is defined as $s(f) = \max\{s(f,x) : x \in \{0,1\}^n\}$.*

▶ **Definition 2.2** (Block Sensitivity). *The block sensitivity $bs(f,x)$ of a Boolean function f on input x is the maximum number of pairwise disjoint subsets $S_1, \ldots, S_k$ of $[n]$ such that for each $i \in [k]$ $f(x) \neq f(x^{S_i})$. The block sensitivity of f is defined as $bs(f) = \max\{bs(f,x) : x \in \{0,1\}^n\}$.*

▶ **Definition 2.3** (Partial assignment, subcube and subfunction). *Given an integer $n > 0$, a partial assignment α is a function $\alpha\colon [n] \to \{0,1,\star\}$. A partial assignment α corresponds naturally to a setting of n variables $(x_1, x_2, \ldots, x_n)$ to $\{0,1,\star\}$ where x_i is set to $\alpha(i)$.*

The variables set to $\star$ are called unassigned or free, and we say that the variables set to 0 or 1 are fixed. We say that $x \in \{0,1\}^n$ agrees with α if $x_i = \alpha(i)$ for all i such that $\alpha(i) \neq \star$. The set of all inputs $x \in \{0,1\}^n$ agreeing with α constitutes a subcube which we denote by $\mathcal{S}_\alpha$.

The size of a partial assignment α is defined as the number of fixed variables of α and denoted as $|\alpha|$.

For a function $f\colon \{0,1\}^n \to \{0,1\}$, we denote by f_α the subfunction obtained by restricting f to the subcube $\mathcal{S}_\alpha$.

▶ **Definition 2.4** (Certificate). *For a function $f\colon \{0,1\}^n \to \{0,1\}$ and input $x \in \{0,1\}^n$ a partial assignment α is a certificate of f on x if x agrees with α, and any input y agreeing with α satisfies $f(y) = f(x)$.*

We denote the set of all certificates of f on x by $\Gamma_f(x)$.

▶ **Definition 2.5** (Certificate Complexity). *The certificate complexity $C(f,x)$ of a Boolean function f on input x is the size of the smallest certificate of f on x. The certificate complexity of f is defined as $C(f) = \max\{C(f,x) : x \in \{0,1\}^n\}$. The minimum certificate complexity of f is defined as $C_{min}(f) = \min\{C(f,x) : x \in \{0,1\}^n\}$.*

▶ **Definition 2.6** (Alternating path). *For a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, an alternating path is defined as any sequence of inputs $x^{(0)}, x^{(1)}, x^{(2)}, \ldots x^{(t)}$, $x^{(i)} \in \{0,1\}^n$ for $i \in \{0,1,\ldots,t\}$, that satisfies the following properties:*

- $x^{(0)} = 0^n$
- $x^{(i)} \prec x^{(i+1)}$ *for all* $i \in \{0,1,\ldots,t-1\}$.
- $f(x^{(i)}) \neq f(x^{(i+1)})$ *for all* $i \in \{0,1,\ldots,t-1\}$

where $a \prec b$ denotes the property that the set of bits set to 1 in a forms a subset of the set of bits set to 1 in b.

▶ **Definition 2.7** (Alternating Number of a function). *For a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, the alternating number of f, $alt(f)$, is defined as the maximum length of any alternating path of f.*

▶ **Definition 2.8** (Invariance Group). *A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is invariant under a permutation $\sigma\colon [n] \to [n]$, if for any $x \in \{0,1\}^n$, $f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$. The set of all permutations under which f is invariant forms a group, called the invariance group of f.*

▶ **Definition 2.9** (Transitive Function). *A Boolean function is transitive if its invariance group Γ is transitive, that is, for each $i,j \in [n]$, there is a $\sigma \in \Gamma$ such that $\sigma(i) = j$.*

For example, the set of all permutations on n bits, denoted by S_n is a transitive group of permutations. Another example of a transitive group of permutations is the set of all *cyclic shifts* on n bits, denoted by $Shift_n = \{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$, where the permutation ξ_j cyclically shifts the string by j positions.

Communication Complexity. We consider a setting with two parties Alice and Bob and a fixed Boolean function $f\colon \{0,1\}^{2n} \to \{0,1\}$. For $x,y \in \{0,1\}^n$, input x is provided to Alice and input y to Bob. Their collective objective is to compute $f(x,y)$.

The communication complexity of f, denoted $CC(f)$, is the maximum value of the minimum number of bits exchanged by Alice and Bob in order to compute $f(x,y)$, where the maximum is taken over all input pairs $(x,y) \in \{0,1\}^{2n}$.

The communication matrix corresponding to f, denoted M_f, is a $2^n \times 2^n$ matrix with rows indexed by all possible values of $x \in \{0,1\}^n$ i.e. Alice's part of the input and columns indexed by all possible values of $y \in \{0,1\}^n$ i.e. Bob's part of the input. It can be shown that $CC(f) \geq \log rank(M_f)$ [23].

The Log-rank conjecture proposed by Lovász and Saks [21] asks whether the communication complexity of a function can also be upper bounded by a polynomial in logarithm of the rank of its communication matrix as:

▶ **Conjecture 2.10.** *For any function $f\colon \{0,1\}^{2n} \to \{0,1\}$,*

$$CC(f) \leq poly(\log rank(M_f))$$

Please see Section A in the Appendix for more definitions and background.

2.1 Previous results

We now state some previous results that we use in our proofs.

First we state a couple of lemmas from a recent paper by Chaubal and Gál [12].

▶ **Lemma 2.11** (Lemma 8 from [12]). *For any non-constant transitive function $f : \{0,1\}^n \to \{0,1\}$, we have $C(f,0^n) \cdot s(f) \geq n$ and $C(f,1^n) \cdot s(f) \geq n$.*

▶ **Lemma 2.12** (Lemma 9 from [12]). *For any non-constant transitive function $f : \{0,1\}^n \to \{0,1\}$, and an integer $5 \leq r \leq 15$, if $C_{min}(f) \leq n^{3/r}$, then $bs(f) \geq \Omega(n^{1-\frac{4}{r}})$.*

We now state a lemma from the paper of Lin and Zhang [20]:

▶ **Lemma 2.13** (Lemma 12 from [20]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, the following two statements hold:*

$$\max\{C(f,0^n), C(f,1^n)\} \leq alt(f) \cdot s(f)$$

$$\max\{C(f,0^n), C(f,1^n)\} \leq alt(f) \cdot deg_2(f)$$

We include more details about the approach and previous results of Lin and Zhang [20] in Section A.1 in the Appendix.

3 Diameters of Boolean functions

We begin with some notation. For the Boolean cube $\mathcal{B}_n$, a path is any sequence of inputs $x^{(0)}, x^{(1)}, x^{(2)}, \ldots, x^{(t)}$ where $x^{(i)} \in \{0,1\}^n$ for $i \in \{0,1,\ldots,t\}$. We define the length of such a path to be the number of steps t. For a path $x^{(0)}, x^{(1)}, x^{(2)}, \ldots, x^{(t)}$, we define a sequence of partial assignments $\{\beta^{(0)}, \beta^{(1)}, \ldots \beta^{(t-1)}\}$ where $\beta^{(i)}\colon [n] \to \{0,1,\star\}$ is defined as follows: $\beta^{(i)}_j = x^{(i)}_j$ for all $j \in [n]$ such that $x^{(i)}_j = x^{(i+1)}_j$ and $\beta^{(i)}_j = \star$ otherwise.

Note that we can view each step $x^{(i)} \to x^{(i+1)}$ on a path as flipping the bits where $x^{(i)}$ and $x^{(i+1)}$ differ. The free variables of the partial assignment $\beta^{(i)}$ are exactly these bits. Thus, for a Boolean function f, the subfunction $f_{\beta^{(i)}}$ depends on the bits where $x^{(i)}$ and $x^{(i+1)}$ differ.

▶ **Definition 3.1** ($\mathcal{H}$-distance between an input and a certificate). *Let $\mathcal{H}$ be a class of Boolean functions. For a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, input $x \in \{0,1\}^n$ and a partial assignment $\alpha\colon [n] \to \{0,1,\star\}$ corresponding to a subcube where f is constant, we define an $\mathcal{H}$-path from x to α as any path $x^{(0)}, x^{(1)}, \ldots x^{(t)}$ that satisfies the following properties:*

- $x^{(0)} = x$
- $x^{(t)}$ *agrees with* α
- *The subfunction $f_{\beta^{(i)}}$ belongs to class $\mathcal{H}$ for each $i \in \{0,1,\ldots,t-1\}$.*

We define the $\mathcal{H}$-distance between x and α with respect to f, denoted $dist_{f,\mathcal{H}}(x,\alpha)$, to be the length of a shortest $\mathcal{H}$-path from x to α.

▶ **Definition 3.2** ($\mathcal{H}$-diameter of a function). *For a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, input $x \in \{0,1\}^n$, and a class of Boolean functions $\mathcal{H}$, we use the notation*

$$dia_{\mathcal{H}}(f,x) = \min_{\alpha \in \Gamma_f(x)} dist_{f,\mathcal{H}}(\bar{x},\ \alpha)\ .$$

Recall that $\bar{x}$ denotes the complement of x and $\Gamma_f(x)$ denotes the set of all certificates of f on x.

We define the $\mathcal{H}$-diameter of f as:

$$dia_{\mathcal{H}}(f) = \max_{x \in \{0,1\}^n} dia_{\mathcal{H}}(f,x)\ .$$

In this work, we will be concerned with the $\mathcal{H}$-diameter of functions for the following classes $\mathcal{H}$:

- AND diameter denoted $dia_\wedge(f)$: Corresponds to the class $\mathcal{H}$ that includes the function AND and its negation the NAND function.
- Sensitivity diameter denoted $dia_s(f)$: Defined by the class $\mathcal{H}$ with functions that have sensitivity equal to the number of input variables.
- Real degree diameter denoted as $dia_{deg}(f)$: Corresponding to the class of functions $\mathcal{H}$ with real degree equal to the number of input variables.
- $\mathbb{F}_2$-degree diameter denoted as $dia_{deg_2}(f)$: Defined by the class $\mathcal{H}$ that include functions with $\mathbb{F}_2$-degree equal to the number of variables.

Note that since the functions AND and NAND belong to each of the classes we consider in this paper, and since $deg_2(f) \leq deg(f)$ for any Boolean function f, we have

$$dia_s(f) \leq dia_\wedge(f) \tag{1}$$

and

$$dia_{deg}(f) \leq dia_{deg_2}(f) \leq dia_\wedge(f) \tag{2}$$

Similarly to minimum certificate complexity, we also define the minimum version of the diameter:

▶ **Definition 3.3** (Min $\mathcal{H}$-diameter of a function)**.** *For a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ and a class of Boolean functions $\mathcal{H}$, we define the min $\mathcal{H}$-diameter of f as:*

$$dia_{min,\mathcal{H}}(f) = \min_{x\in\{0,1\}^n} dia_{\mathcal{H}}(f,x)\ .$$

and we define the closure of the min $\mathcal{H}$-diameter of f as:

$$dia^{clo}_{min,\mathcal{H}}(f) = \max_{\alpha} dia_{min,\mathcal{H}}(f_\alpha)$$

where the maximum is taken over all possible partial assignments α on n variables, or in other words, over all possible subfunctions f_α of f.

Note that for any function f and class $\mathcal{H}$, we have $dia_{min,\mathcal{H}}(f) \leq dia^{clo}_{min,\mathcal{H}}(f) \leq dia_{\mathcal{H}}(f)$.

3.1 Upper bounds on diameters

▶ **Lemma 3.4.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

$$dia_\wedge(f) \leq 2C(f)$$

Proof. For any input $x \in \{0,1\}^n$, we shall prove that $dia_\wedge(f,x) \leq 2C(f,x)$.

Let α be a certificate of f on x achieving $|\alpha| = C(f,x)$. We shall construct an AND-NAND path $x^{(0)}, x^{(1)}, \ldots x^{(t)}$ from $\bar{x}$ to α, with length $t \leq 2|\alpha|$.

We start with $x^{(0)} = \bar{x}$ as required. We now give an inductive description of our construction. Let us assume that we have found the first $i+1$ vertices of the path i.e. $x^{(0)}, x^{(1)}, \ldots x^{(i)}$. Then we get the next vertex $x^{(i+1)}$ in the following way based on the value of $f(x^{(i)})$:

1. Case 1: $f(x^{(i)}) = f(x)$
   If $x^{(i)}$ agrees with α, then we have successfully found the required $\mathcal{H}$-path from $\bar{x}$ to α and we can stop.
   Otherwise, if $x^{(i)}$ does not agree with α, then we choose $x^{(i+1)} = (x^{(i)})^S$ where S is any minimal sensitive block of f on $x^{(i)}$ such that S does not contain any index where $x^{(i)}$ and α agree. Note that such a block S must exist because otherwise, the set of bits where $x^{(i)}$ and α agree would be a certificate of f, which would contradict the minimality of the certificate α.
   We note that in this case, $x^{(i+1)}$ agrees with α on at least as many bits as $x^{(i)}$ agrees with α.
2. Case 2: $f(x^{(i)}) \neq f(x)$
   In this case, we first observe that the set T of all the bits where $x^{(i)}$ and α disagree constitutes a sensitive block for f on $x^{(i)}$. Therefore, there exists a subset $S \subset T$ which is a minimal sensitive block of f on $x^{(i)}$. We then choose $x^{(i+1)} = (x^{(i)})^S$.
   Note that the number of bits where $x^{(i+1)}$ agrees with α is strictly greater than the number of bits where $x^{(i)}$ agrees with α.

First we note that since each step consists of flipping a minimal sensitive block, each of the subfunctions $f_{\beta^{(i)}}$ is either AND or NAND: Recall that the subfunction $f_{\beta^{(i)}}$ depends on the bits where $x^{(i)}$ and $x^{(i+1)}$ differ. So for example, if $f(x^{(i)}) = 0$, then the subfunction $f_{\beta^{(i)}}$ is 0 everywhere except when all its free variables agree with $x^{(i+1)}$.

Further, since an AND-NAND path is also an alternating path, the value of $f(x^{(i)})$ alternates between 0 and 1. Therefore, the above described procedure to construct the AND-NAND path alternates between case 1 and case 2.

Also, as noted before, the number of bits where $x^{(i+1)}$ agrees with α is strictly greater than the number of bits where $x^{(i)}$ agrees with α in case 2, whereas in case 1, we can guarantee that this number does not decrease. Since the procedure alternates between the two cases, $x^{(i+2)}$ must agree with α on at least one more bit than $x^{(i)}$, for $i \in \{0, 1, \ldots t-2\}$. Therefore, the procedure must terminate in at most $2|\alpha|$ steps, implying that $t \leq 2|\alpha|$. ◀

Next, note that since each of our measures is upper bounded by certificate complexity (as we proved above), known upper bounds on certificate complexity imply that for each class $\mathcal{H}$ considered in this paper, we have $dia_{\mathcal{H}}(f) \leq O(s(f)^5)$ (using Huang's result [17]) and $dia_{\mathcal{H}}(f) \leq O(deg(f)^3)$ by [24].

Improving these upper bounds would have interesting consequences, as we described in the introduction.

3.2 Upper bounds on certificate complexity in terms of diameters

▶ **Lemma 3.5.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$ and input $x \in \{0,1\}^n$, we have:*

$$C(f,x) \leq dia_s(f,x) \cdot s(f) \leq dia_\wedge(f,x) \cdot s(f) \tag{3}$$

$$C(f,x) \leq dia_{deg}(f,x) deg(f) \leq dia_\wedge(f,x) \cdot deg(f) \tag{4}$$

$$C(f,x) \leq dia_{deg_2}(f,x) deg_2(f) \leq dia_\wedge(f,x) \cdot deg_2(f) \tag{5}$$

Proof. We shall first prove inequality 3.

Let α be a certificate of f on x and $x^{(0)}, x^{(1)}, \ldots, x^{(t)}$ be a corresponding full sensitivity path from $\bar{x}$ to α that achieves the minimum value of $dist_{f,s}(\bar{x}, \alpha)$.

Then note that every fixed bit of the certificate α must be contained in $\beta^{(i)}$ for some $i \in \{0, 1, \ldots, t-1\}$ since $x^{(t)}$ agrees with α and $x^{(0)}$ (i.e. $\bar{x}$) disagrees with all the fixed bits of α.

Therefore, $|\beta^{(0)}| + |\beta^{(1)}| + \ldots + |\beta^{(t-1)}| \geq |\alpha|$. So there must exist an $i \in \{0, 1, \ldots, t-1\}$ such that $|\beta^{(i)}| \geq \frac{|\alpha|}{t}$. Now consider the subfunction $f_{\beta^{(i)}}$. Since we considered a full sensitivity path, this subfunction has sensitivity $|\beta^{(i)}|$. Therefore, $s(f) \geq |\beta^{(i)}| \geq \frac{|\alpha|}{t}$.

This implies that $s(f) \cdot dist_{f,s}(\bar{x}, \alpha) \geq |\alpha|$.

Taking the minimum over all the certificates for f on x gives the first part of inequality 3. The second part follows due to inequality 1. The other two inequalities follow by an analogous argument. ◀

Lemma 3.5 immediately implies the following two theorems.

▶ **Theorem 3.6.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

1. $C(f) \leq dia_s(f) \cdot s(f) \leq dia_\wedge(f) \cdot s(f)$
2. $C(f) \leq dia_{deg}(f) \cdot deg(f) \leq dia_\wedge(f) \cdot deg(f)$
3. $C(f) \leq dia_{deg_2}(f) \cdot deg_2(f) \leq dia_\wedge(f) \cdot deg_2(f)$.

Proof. Let x be the input achieving $C(f, x) = C(f)$. Then, equation 3 gives:

$$\begin{aligned} C(f) &= C(f, x) \\ &\leq dia_s(f, x) \cdot s(f) \\ &\leq dia_s(f) \cdot s(f). \end{aligned}$$

This gives the first part of the first statement of the theorem, the second part follows by equation 1. The other statements follow similarly from Lemma 3.5 and equation 2. ◀

▶ **Theorem 3.7.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

1. $C_{min}(f) \leq dia_{min,s}(f) \cdot s(f) \leq dia_{min,\wedge}(f) \cdot s(f)$
2. $C_{min}(f) \leq dia_{min,deg}(f) \cdot deg(f) \leq dia_{min,\wedge}(f) \cdot deg(f)$
3. $C_{min}(f) \leq dia_{min,deg_2}(f) \cdot deg_2(f) \leq dia_{min,\wedge}(f) \cdot deg_2(f)$.

Proof. Let x be the input for which the minimum value of $dia_s(f, x)$ is achieved. Then, equation 3 gives:

$$\begin{aligned} C_{min}(f) &\leq C(f, x) \\ &\leq dia_s(f, x) \cdot s(f) \\ &= dia_{min,s}(f) \cdot s(f). \end{aligned}$$

The first statement of the theorem follows.

Similarly equations 4 and 5, respectively, imply the second and third statements of the theorem. ◀

4 Results for families of functions with small diameters

4.1 Transitive functions with small diameters

In this section, we improve the lower bounds on sensitivity of transitive functions with constant alternating number that follow from the work of Lin and Zhang [20] and then also prove a similar result for transitive functions with constant AND diameter. We then proceed to prove lower bounds on block sensitivity of transitive functions with constant minimum AND diameter.

▶ **Lemma 4.1.** *For any non-constant transitive function* $f\colon \{0,1\}^n \to \{0,1\}$ *the following two statements hold:*

$$s(f)^2 \cdot alt(f) \geq n$$

$$s(f) \cdot deg_2(f) \cdot alt(f) \geq n$$

Proof. Recall that Lemma 2.11 gives that:

$$C(f, 0^n)s(f) \geq n$$

The first part of Lemma 2.13 gives that:

$$C(f, 0^n) \leq alt(f) \cdot s(f)$$

Together they imply the first statement of the lemma.

The second statement follows similarly using the second part of Lemma 2.13. ◀

Note that this implies $s(f) \geq \sqrt{n}$ for transitive functions with constant alternating number, giving the best possible bound for such functions.

The first statement of Lemma 4.1 is tight for the TRIBES function on n variables: TRIBES is monotone and therefore has $alt(f) = 1$. Also, TRIBES is transitive as noted in [30]. It is easy to see that TRIBES has $s(f) = \sqrt{n}$.

▶ **Lemma 4.2.** *For any non-constant transitive function* $f\colon \{0,1\}^n \to \{0,1\}$ *the following two statements hold:*

$$s(f)^2 \cdot dia_\wedge(f) \geq n,$$

$$s(f) \cdot deg_2(f) \cdot dia_\wedge(f) \geq n.$$

Proof. Recall that Lemma 2.11 gives that:

$$C(f, 0^n)s(f) \geq n$$

Further equation 3 gives that:

$$C(f, 0^n) \leq dia_\wedge(f, 0^n) \cdot s(f)$$

Therefore, we get:

$$dia_\wedge(f, 0^n) \cdot s(f)^2 \geq n$$

which implies the first part of the lemma.

A similar argument gives the second part of the lemma using equation 5. ◀

▶ **Corollary 4.3.** *For any non-constant transitive function* $f\colon \{0,1\}^n \to \{0,1\}$ *with constant alternating number or constant AND diameter* $dia_\wedge(f) = O(1)$*, we have:*

$$s(f) \geq \Omega(\sqrt{n})$$

We now prove a lower bound on the block sensitivity of transitive functions under the weaker condition of having constant minimum AND diameter.

▶ **Lemma 4.4.** *For any non-constant transitive function* $f\colon \{0,1\}^n \to \{0,1\}$ *with* $dia_{min,\wedge}(f) = O(1)$*, we have:*

$$bs(f) \geq \Omega(n^{3/7})$$

Proof. We have two cases:

Case 1: $C_{min}(f) \geq n^{3/7}$. The first part of Theorem 3.7 implies that $C_{min}(f) \leq dia_{min,\wedge}(f) \cdot s(f) \leq O(s(f))$, since $dia_{min,\wedge}(f) = O(1)$.

Then $n^{3/7} \leq C_{min}(f) \leq O(s(f)) \leq O(bs(f))$ and we are done.

Case 2: $C_{min}(f) \leq n^{3/7}$. Now we use Lemma 2.12 with $r = 7$. This implies that if any transitive function f has $C_{min}(f) \leq n^{3/7}$, then $bs(f) \geq n^{3/7}$, implying the statement of the Lemma in this case. ◀

4.2 Implications to the log-rank conjecture for XOR functions

For any $f\colon \{0,1\}^n \to \{0,1\}$, the corresponding XOR function $f \circ \oplus\colon \{0,1\}^{2n} \to \{0,1\}$ is defined as: $f \circ \oplus(x,y) = f(x \oplus y)$, where $x \oplus y$ is the bitwise XOR of $x, y \in \{0,1\}^n$.

Lin and Zhang [20] proved that the log-rank conjecture holds for XOR functions $f \circ \oplus$ such that $alt(f)$ is at most polynomial in $\log ||\hat{f}||_0$ (see Theorem A.11).

In this section, we prove that the log-rank conjecture holds for functions of the form $f(x \oplus y)$ such that the $\mathbb{F}_2$-degree diameter of f is upper bounded by a polynomial in the logarithm of the Fourier sparsity of f.

First we prove an analogous result to Theorem A.11 implying the log-rank conjecture for XOR functions with bounded $\mathbb{F}_2$-degree diameter. In contrast to the proof of Theorem A.11, we do not need to upper bound $C^{clo}_{min}(f)$, since Theorem 3.6 proves an upper bound directly on $C(f)$ in terms of the product of $dia_{deg_2}(f)$ and $deg_2(f)$ for any function f. This gives us the following result confirming the log-rank conjecture for functions $f \circ \oplus$ with $dia_{deg_2}(f)$ upper bounded by a polynomial in the logarithm of the Fourier sparsity of f:

▶ **Theorem 4.5.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

$$CC(f \circ \oplus) \leq 2dia_{deg_2}(f) \log^2 rank(M_{f\circ\oplus})$$

Proof. Recall the third statement of Theorem 3.6 which states that:

$$C(f) \leq dia_{deg_2}(f) \cdot deg_2(f)$$

Along with Lemma A.10, we get that:

$$\begin{aligned} CC(f \circ \oplus) &\leq 2C(f) \cdot \log rank(M_{f\circ\oplus}) \\ &\leq 2dia_{deg_2}(f) \cdot deg_2(f) \cdot \log rank(M_{f\circ\oplus}) \\ &\leq 2dia_{deg_2}(f) \cdot \log^2 rank(M_{f\circ\oplus}) \end{aligned}$$

Here the last inequality follows from Lemmas A.6 and A.9. ◀

We note that the statement of Theorem 4.5 also holds with $dia_\wedge(f)$ replacing $dia_{deg_2}(f)$, since the $\mathbb{F}_2$-degree diameter is upper bounded by the AND diameter for any function f as noted in equation 2. We state Theorem 4.5 with $dia_{deg_2}(f)$ instead of $dia_\wedge(f)$ because it gives a stronger statement since there exist functions with dia_{deg_2} much smaller than $dia_\wedge$ as illustrated by Example 5.2.

Next we prove a common strengthening of Theorem A.11 and Theorem 4.5. We show that the communication complexity of a function of the form $f(x \oplus y)$ can also be upper bounded in terms of the closure of its min $\mathbb{F}_2$-degree diameter and the square of the log of rank of its communication matrix $M_{f\circ\oplus}$.

▶ **Theorem 4.6.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$:*

$$CC(f \circ \oplus) \leq 2dia^{clo}_{min,deg_2}(f) \cdot \log^2 rank(M_{f\circ\oplus})$$

Proof. From the third statement of Theorem 3.7, we have that:

$$C^{clo}_{min}(f) \leq dia^{clo}_{min,deg_2}(f) \cdot deg_2(f)$$

Combining this with Lemmas A.6, A.9 and A.10 gives the result. ◀

As we shall note in Lemma 4.7, $dia_{min,deg_2}(f) \leq dia_{min,\wedge}(f) \leq alt(f)$. Since alternating number is a downward non-increasing measure, this implies that $dia^{clo}_{min,deg_2}(f) \leq alt(f)$. Furthermore, Example 5.4 gives a family of functions $f\colon \{0,1\}^n \to \{0,1\}$ with alternating number exponentially larger than all our diameters. This shows that Theorem 4.6 is a strictly stronger statement than Theorem A.11.

By definition, we have that for any function f, $dia^{clo}_{min,deg_2}(f) \leq dia_{deg_2}(f)$. Therefore, Theorem 4.6 is a potentially stronger statement than Theorem 4.5. As of now, we are not aware of any example function f separating $dia^{clo}_{min,deg_2}(f)$ from $dia_{deg_2}(f)$. However, we remark that the TRIBES function separates $dia^{clo}_{min,\wedge}(f)$ from $dia_{\wedge}(f)$ as noted in Section 5.8.

We illustrate with examples in Section 5 that, in general, the alternating number of a function and its $\mathcal{H}$-diameter are incomparable for the different classes $\mathcal{H}$ that we consider. However, in the following lemma, we show that the min AND diameter, and consequently, the min $\mathcal{H}$-diameter for all our different classes $\mathcal{H}$, are upper bounded by the alternating number.

▶ **Lemma 4.7.** *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have,*

$$dia_{min,\wedge}(f) \leq alt(f)$$

Proof. We prove the following relationship, which immediately implies the statement of the lemma:

$$dia_{\wedge}(f, 1^n) \leq alt(f) \tag{6}$$

Let $alt(f) = t$ and let $\mathcal{Q} = x^{(0)}, x^{(1)}, \ldots x^{(t)}$ be an alternating path of length t.

Now, we construct an AND-NAND path $\mathcal{Q}' = z^{(0)}, z^{(1)}, \ldots z^{(t)}$ from 0^n to a certificate α of 1^n in the following way:

Let $z^{(0)} = x^{(0)} = 0^n$. Let $z^{(1)} \leq x^{(1)}$ be a minimal element such that $f(z^{(1)}) = f(x^{(1)})$. Recall that by the definition of alternating path, $f(x^{(i)}) \neq f(x^{(i+1)})$. Thus, the set of variables where $z^{(0)}$ and $z^{(1)}$ differ forms a minimal sensitive block for f on $z^{(0)}$: for all $y \neq z^{(1)}$ such that $z^{(0)} \prec y \prec z^{(1)}$, $f(y) = f(z^{(0)})$ but $f(z^{(1)}) \neq f(z^{(0)})$.

In general, for $i \in \{0, 1, \ldots, t-1\}$, let $z^{(i+1)} \prec x^{(i+1)}$ be a minimal element such that $f(z^{(i+1)}) = f(x^{(i+1)})$, and $z^{(i)} \prec z^{(i+1)}$ Thus, the set of variables where $z^{(i)}$ and $z^{(i+1)}$ differ forms a minimal sensitive block for f on $z^{(i)}$. As we noted before (see Section 3.1) subfunctions over a set of variables that forms a minimal sensitive block are either the AND or the NAND function. Thus, for the path $\mathcal{Q}'$, each subfunction f_{β^i} is either an AND or a NAND.

We will thus get an AND-NAND path $z^{(0)}, z^{(1)}, \ldots, z^{(t)}$ of length t. Note that $z^{(t)}$ must agree with some certificate of 1^n, since otherwise, we can get an alternating path for f of length greater than t in the following way: consider the alternating path $\mathcal{Q}' = z^{(0)}, z^{(1)}, \ldots z^{(t)}$. Since $z^{(t)}$ does not agree with any certificate of 1^n, the partial assignment α defined as $\alpha_i = 1$ whenever $z^{(t)}_i = 1$ and $\alpha_i = \star$ otherwise, is not a certificate of f. This implies the existence of an input $z^{(t+1)}$ such that $z^{(t)} \prec z^{(t+1)}$ and $f(z^{(t)}) \neq f(z^{(t+1)})$. Therefore, the path $\mathcal{Q}'' = z^{(0)}, z^{(1)}, \ldots z^{(t)}, z^{(t+1)}$ is an alternating path of length $t+1$ contradicting the fact that $alt(f) = t$.

Therefore, the path $z^{(0)}, z^{(1)}, \ldots, z^{(t)}$ is an AND-NAND path from 0^n to some certificate of f on 1^n and the statement follows. ◀

5 Separating Examples

In this section, we give several examples, separating various types of diameters from alternating number and from each other.

5.1 Separating $dia_s(f)$ from $dia_\wedge(f)$

The following example has constant sensitivity diameter, whereas its AND diameter equals the number of input variables.

▶ **Example 5.1.** Let $f\colon \{0,1\}^n \to \{0,1\}$ be the PARITY function on n bits i.e. $PARITY(x) = \bigoplus_{i\in[n]} x_i$.

It is easy to see that $dia_\wedge(PARITY) = n$, since for any partial assignment α, the subfunction $PARITY_\alpha$ belongs to the AND-NAND class only if α fixes all but 1 variable.

On the other hand, for any input $x \in \{0,1\}^n$, $dia_s(PARITY, x) = 1$. This is because we can consider α to be the certificate fixing all the bits of x and then the path $\bar{x}, x$ is a valid $\mathcal{H}$-path since $s(PARITY) = n$ (i.e. $PARITY$ induced on the "entire cube" has full sensitivity).

5.2 Separating $dia_{deg}(f)$ (and also $dia_{deg_2}(f)$) from $dia_\wedge(f)$

The next example has constant values for both its real degree diameter as well as $\mathbb{F}_2$-degree diameter, but has large AND diameter.

▶ **Example 5.2.** Define $f\colon \{0,1\}^n \to \{0,1\}$ as follows:
$f(0^n) = 1$,
$f(x) = \bigoplus_{i\in[n]} x_i$ otherwise.

It is easy to show that $dia_\wedge(f) = n$ by a similar argument as in example 5.1.

Also, we note that $\deg_2(f) = n$. This follows from a result of Beigel and Bernasconi [4], stating that for any Boolean function, $deg_2(f) = n$ iff $|f^{-1}(1)|$ is odd.

Therefore, by an analogous argument as in example 5.1, for any input $x \in \{0,1\}^n$, $dia_{deg_2}(f, x) = 1$. (We can again consider α to be the certificate fixing all the bits of x and the path $\bar{x}, x$ is a valid $\mathcal{H}$-path since $deg_2(f) = n$.)

Therefore, we have $dia_{deg_2}(f) = 1$.

We also have that for any Boolean function f, $deg_2(f) \leq deg(f)$ (see for example, proposition 6.23 in [30]).

Therefore, $deg(f) = n$, and by a similar argument as for the $\mathbb{F}_2$-degree, $dia_{deg}(f) = 1$.

We note that the PARITY function from example 5.1 also separates $dia_{deg}(f)$ from $dia_\wedge(f)$. This is because $dia_{deg}(PARITY) = 1$ as we discuss below, whereas $dia_\wedge(PARITY) = n$ as noted in Example 5.1.

5.3 Separating $dia_{deg}(f)$ from $dia_{deg_2}(f)$

Recall from equation 2 that $dia_{deg}(f) \leq dia_{deg_2}(f)$ for any boolean function f. To separate $dia_{deg}(f)$ from $dia_{deg_2}(f)$, we consider again the PARITY function discussed in Example 5.1. It is easy to see that $deg_2(PARITY) = 1$. Moreover, for any partial assignment $\alpha\colon [n] \to \{0,1,\star\}$, the subfunction $PARITY_\alpha$ is also a PARITY function on the free bits and therefore, $deg_2(PARITY_\alpha) = 1$. So we have $dia_{deg_2}(PARITY) = n$. However, $deg(PARITY) = n$, by the characterization due to Shi and Yao (see in the survey [9]) which states that for

any function $f\colon \{0,1\}^n \to \{0,1\}$, $deg(f) = n$ iff the number of 1-inputs with an even number of 1's does not equal the number of 1-inputs with an odd number of 1's. Therefore, $dia_{deg}(PARITY) = 1$.

5.4 Separating $dia_s(f)$ and $dia_{deg_2}(f)$ from each other

The measures $dia_s(f)$ and $dia_{deg_2}(f)$ are incomparable, and we provide examples separating them in both directions.

We again revisit the PARITY function considered in Example 5.1 to illustrate a function with small $dia_s(f)$ and large $dia_{deg_2}(f)$. As noted before, $dia_{deg_2}(PARITY) = n$, whereas $dia_s(PARITY) = 1$, achieving the required separation.

To illustrate a separation in the other direction, we consider the TRIBES function on n^2 bits that has $dia_s(TRIBES) = \Theta(n)$ as we shall see in Example 5.3. However, $deg_2(TRIBES) = n^2$ and therefore, $dia_{deg_2}(TRIBES) = 1$.

5.5 Separating $dia_s(f)$ from $dia_{deg}(f)$

We now mention a separating example with $dia_{deg}(f)$ much smaller than $dia_s(f)$. The TRIBES function (see also Example 5.3) on n^2 bits has $dia_s(TRIBES) = \Theta(n)$. However, $deg(TRIBES) = n^2$ and therefore, $dia_{deg}(TRIBES) = 1$.

We are not aware of any examples as yet, separating these measures in the other direction. We do believe these measures to be incomparable, and it would be an interesting exercise to find functions f with $dia_s(f)$ asymptotically smaller than $dia_{deg}(f)$.

5.6 Example with $alt(f)$ smaller than $dia_s(f)$ (and also $dia_\wedge(f)$)

We now present an example where the alternating number is much smaller than $dia_\wedge(f)$ as well as $dia_s(f)$.

▶ **Example 5.3.** Consider the TRIBES function $f\colon \{0,1\}^{n^2} \to \{0,1\}$ defined as:

$$TRIBES(x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}, \ldots, x_{n1}, \ldots x_{nn}) = \bigvee_{i\in[n]} \bigwedge_{j\in[n]} x_{ij}$$

We first note that since $TRIBES$ is monotone, $alt(TRIBES) = 1$.

We shall show that $dia_\wedge(TRIBES) \geq 2n - 1$.

Consider the 1-input $x = 1^n(0^2 1^{n-2})^{n-1}$. In other words, the first block of n bits of x are set to 1, the remaining $n-1$ blocks of n bits each have the first 2 bits set to 0 and the rest set to 1.

Note that $TRIBES(\bar{x}) = 0$.

Now, let $x^{(0)}, x^{(1)}, \ldots, x^{(t)}$ be any valid AND-NAND path from x to α where α is a certificate of $\bar{x}$. (Note that we have switched the roles of x and $\bar{x}$ in this example for convenience.)

Since $TRIBES(x^{(0)}) \neq f(x^{(1)}) = 0$, the partial assignment $\beta^{(0)}$ must have free bits belonging to the first block of n bits, and moreover, it cannot contain any free bits from any of the other blocks, in order for the function $TRIBES_{\beta^{(0)}}$ to belong to the AND-NAND class.

For the next step, since $TRIBES(x^{(2)}) = 1$, it is necessary that both 0-bits must be flipped from one of the remaining blocks. In other words, the partial assignment $\beta^{(1)}$ must have exactly two free variables corresponding to the first two bits of some block (other than the first block).

Again, as before, the partial assignment $\beta^{(2)}$ must contain free variables from the block which now only contains 1-bits.

In this way, any shortest valid AND-NAND path must alternate between changing some block to contain only 1-bits (thereby changing the function value to 1), and then flipping some 1-bit in that block to 0 (changing the function value to 0).

Eventually, every block will contain a bit that was flipped from a 1 to a 0, and the set of these bits shall constitute a certificate of $\bar{x}$.

Therefore, we have that $dia_\wedge(TRIBES) \geq 2n - 1$. We note that this bound is tight up to constant factors, as can be seen from Theorem B.1 which implies that $dia_\wedge(TRIBES) \leq O(n)$.

A similar argument also works to show that $dia_s(TRIBES) \geq 2n - 1$, and therefore, $dia_s(TRIBES) = \theta(n)$ due to Theorem B.1.

However, since $deg(TRIBES) = n^2$, we have that $dia_{deg}(TRIBES) = 1$.

Similarly, $deg_2(TRIBES) = n^2$ and therefore, $dia_{deg_2}(TRIBES) = 1$.

5.7 Example with $alt(f)$ larger than all our diameters

We refer to an example from [13] that separates $alt(f)$ from $C(f)$ (and consequently, from all of our diameters).

▶ **Example 5.4.** Let f be the function constructed in [13] as an example where $alt(f)$ is exponentially larger than $DT(f)$ and therefore also $C(f)$ (since $DT(f) \geq C(f)$). We note that since $dia_\wedge(f) \leq 2C(f)$ due to Lemma 3.4, f also acts as a separating example where $alt(f)$ is exponentially larger than $dia_\wedge(f)$, and therefore, also exponentially larger than $dia_s(f), dia_{deg_2}(f)$ and $dia_{deg}(f)$.

5.8 Separating $dia^{clo}_{min,\wedge}(f)$ from $dia_\wedge(f)$ and $dia^{clo}_{min,s}(f)$ from $dia_s(f)$

For separating $dia^{clo}_{min,\wedge}(f)$ from $dia_\wedge(f)$, we revisit the TRIBES function considered in Example 5.3. As noted in that example, $dia_\wedge(TRIBES) = \Theta(n)$. On the other hand, we have that $dia^{clo}_{min,\wedge}(TRIBES) \leq alt(TRIBES) = 1$, thereby achieving the required separation. The same separation is also achieved for the TRIBES function between $dia^{clo}_{min,s}(f)$ and $dia_s(f)$ by an analogous argument.

References

1 Scott Aaronson, Shalev Ben-David, Robin Kothari, and Avishay Tal. Quantum Implications of Huang's Sensitivity Theorem. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:66, 2020. URL: https://eccc.weizmann.ac.il/report/2020/066.

2 Kazuyuki Amano. Minterm-transitive functions with asymptotically smallest Block Sensitivity. *Inf. Process. Lett.*, 111(23-24):1081–1084, 2011. doi:10.1016/j.ipl.2011.09.008.

3 Kaspars Balodis. Several Separations Based on a Partial Boolean Function. *arXiv e-prints*, March 2021. arXiv:2103.05593.

4 Richard Beigel and Anna Bernasconi. A note on the polynomial representation of boolean functions over GF(2). *International Journal of Foundations of Computer Science*, 10(04):535–542, 1999. doi:10.1142/S012905419900037X.

5 Shalev Ben-David, Mika Goos, Siddhartha Jain, and Robin Kothari. Unambiguous DNFs from HEX. *arXiv e-prints*, February 2021. arXiv:2102.08348.

6 Shalev Ben-David, Pooya Hatami, and Avishay Tal. Low-Sensitivity Functions from Unambiguous Certificates. In *Proceedings of Innovations in Theoretical Computer Science Conference (ITCS)*, pages 28:1–28:23, 2017. doi:10.4230/LIPIcs.ITCS.2017.28.

7 A. Bernasconi and B. Codenotti. Spectral analysis of boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345–351, 1999.

8 Eric Blais, Clément L Canonne, Igor C Oliveira, Rocco A Servedio, and Li-Yang Tan. Learning circuits with few negations. *arXiv preprint*, 2014. arXiv:1410.8420.

9 Harry Buhrman and Ronald De Wolf. Complexity Measures and Decision Tree Complexity: A Survey. *Theoretical Computer Science*, 288(1):21–43, 2002. doi:10.1016/S0304-3975(01)00144-X.

10 Sourav Chakraborty. On the Sensitivity of Cyclically-Invariant Boolean functions. *Discrete Mathematics & Theoretical Computer Science*, 13(4):51–60, 2011. URL: http://dmtcs.episciences.org/552.

11 J.-C Chang and H.-L Wu. The log-rank conjecture for read-k xor functions. *Journal of Information Science and Engineering*, 34:391–399, March 2018.

12 Siddhesh Chaubal and Anna Gál. Tight bounds on sensitivity and block sensitivity of some classes of transitive functions. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:134, 2020. URL: https://eccc.weizmann.ac.il/report/2020/134/.

13 Krishnamoorthy Dinesh and Jayalal Sarma. Alternation, Sparsity and Sensitivity: Combinatorial Bounds and Exponential Gaps. In *Proceedings of the 4th International Conference on Algorithms and Discrete Applied Mathematics (CALDAM)*, pages 260–273, 2018. doi:10.1007/978-3-319-74180-2_22.

14 Krishnamoorthy Dinesh and Jayalal Sarma. Sensitivity, affine transforms and quantum communication complexity. In *Computing and Combinatorics - 25th International Conference, COCOON 2019, Proceedings*, volume 11653 of *Lecture Notes in Computer Science*, pages 140–152. Springer, 2019.

15 Andrew Drucker. Block Sensitivity of Minterm-Transitive functions. *Theor. Comput. Sci.*, 412(41):5796–5801, 2011. doi:10.1016/j.tcs.2011.06.025.

16 Siyao Guo, Tal Malkin, Igor C. Oliveira, and Alon Rosen. The power of negations in cryptography. In *Theory of Cryptography*, pages 36–65, 2015.

17 Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019.

18 Raghav Kulkarni and Miklos Santha. Query complexity of matroids. In Paul G. Spirakis and Maria Serna, editors, *Algorithms and Complexity*, pages 300–311, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

19 Sophie Laplante, Reza Naserasr, and Anupa Sunny. Sensitivity Lower Bounds from Linear Dependencies. In *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 62:1–62:14, 2020. doi:10.4230/LIPIcs.MFCS.2020.62.

20 Chengyu Lin and Shengyu Zhang. Sensitivity Conjecture and Log-Rank Conjecture for Functions with Small Alternating Numbers. In *Proceedings of the 44th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 51:1–51:13, 2017. doi:10.4230/LIPIcs.ICALP.2017.51.

21 László Lovász and Michael Saks. Lattices, mobius functions and communications complexity. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 81–90. IEEE Computer Society, 1988.

22 A. A. Markov. On the inversion complexity of a system of functions. *J. ACM*, 5(4):331–334, October 1958. doi:10.1145/320941.320945.

23 Kurt Mehlhorn and Erik M. Schmidt. Las vegas is better than determinism in vlsi and distributed computing (extended abstract). In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, STOC '82, page 330–337. Association for Computing Machinery, 1982. doi:10.1145/800070.802208.

24 Gatis Midrijanis. Exact quantum query complexity for total boolean functions. *arXiv preprint*, 2004. arXiv:quant-ph/0403168.

25 Ashley Montanaro and Tobias Osborne. On the communication complexity of XOR functions. *CoRR*, abs/0909.3392, 2009. arXiv:0909.3392.

26 Hiroki Morizumi. Limiting negations in formulas. In *Proceedings of the 36th International Colloquium on Automata, Languages and Programming: Part I*, ICALP '09, page 701–712. Springer-Verlag, 2009. doi:10.1007/978-3-642-02927-1_58.

27 Hiroki Morizumi. Limiting negations in non-deterministic circuits. *Theoretical Computer Science*, 410(38):3988–3994, 2009. doi:10.1016/j.tcs.2009.05.018.

28 Noam Nisan and Mario Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, December 1994. doi:10.1007/BF01263419.

29 Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Comb.*, 15(4):557–565, 1995. doi:10.1007/BF01192527.

30 Ryan O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, 2014.

31 Miklos Santha and Christopher Wilson. Limiting negations in constant depth circuits. *SIAM Journal on Computing*, 22(2):294–302, 1993. doi:10.1137/0222022.

32 Xiaoming Sun. Block Sensitivity of Weakly Symmetric Functions. In *Proceedings of the Third International Conference on Theory and Applications of Models of Computation (TAMC)*, pages 339–344, 2006. doi:10.1007/11750321_32.

33 Xiaoming Sun. An improved lower bound on the Sensitivity Complexity of Graph Properties. *Theor. Comput. Sci.*, 412(29):3524–3529, 2011. doi:10.1016/j.tcs.2011.02.042.

34 Shao Chin Sung and Keisuke Tanaka. Limiting negations in bounded-depth circuits: An extension of markov's theorem. In *Algorithms and Computation*, pages 108–116. Springer, 2003.

35 H. Y. Tsang, C. H. Wong, N. Xie, and S. Zhang. Fourier sparsity, spectral norm, and the log-rank conjecture. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 658–667, 2013.

36 Hing Yin Tsang. On boolean functions with low sensitivity. *Manuscript*, 2014. URL: http://theorycenter.cs.uchicago.edu/REU/2014/final-papers/tsang.pdf.

37 Hing Yin Tsang, Chung Hoi Wong, Ning Xie, and Shengyu Zhang. Fourier Sparsity, Spectral Norm, and the Log-Rank Conjecture. In *54th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 658–667, 2013. doi:10.1109/FOCS.2013.76.

38 Gyorgy Turan. The Critical Complexity of Graph Properties. *Information Processing Letters*, 18(3):151–153, 1984. doi:10.1016/0020-0190(84)90019-X.

39 Zhiqiang Zhang and Yaoyun Shi. Communication complexities of symmetric xor functions. *Quantum Info. Comput.*, 9(3):255–263, 2009.

A Further Background

▶ **Definition A.1** (Real degree of a function). *A polynomial p over the reals with n variables is said to represent a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ if $p(x) = f(x)$ for all $x \in \{0,1\}^n$. The degree of the unique multilinear polynomial over the reals representing f is defined to be the* degree *of f, and is denoted as $deg(f)$.*

▶ **Definition A.2** ($\mathbb{F}_2$ degree of a function). *For any Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, the degree of the unique multilinear polynomial over $\mathbb{F}_2$ representing f is called as the $\mathbb{F}_2$ degree of f, denoted $deg_2(f)$.*

▶ **Definition A.3** (Decision tree complexity). *A decision tree evaluating a function $f\colon \{0,1\}^n \to \{0,1\}$ is a rooted binary tree with internal nodes labeled by variables and leaves labeled by $\{0,1\}$. The depth of a decision tree is defined as the length of a longest root to leaf path in the tree.*

For any input $x \in \{0,1\}^n$, the label at the leaf reached by following the decision tree queries is the evaluation of the decision tree on x. The decision tree is said to compute the function f if it evaluates to $f(x)$ on every input $x \in \{0,1\}^n$. The decision tree complexity of a boolean function f, denoted $DT(f)$, is defined as the smallest possible depth of any decision tree computing f.

▶ **Definition A.4** (Fourier sparsity of a function). *Any function $f\colon \{0,1\}^n \to \{0,1\}$ can be uniquely represented as*

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)(-1)^{\sum_{i \in S} x_i}$$

This is said to be the Fourier expansion of f and the coefficients $\hat{f}(S)$ are called the Fourier coefficients of f. The number of non-zero Fourier coefficients of f is defined to be the Fourier sparsity of f, denoted $||\hat{f}||_0$.

We note that usually the Fourier representation is considered for functions of the form $f\colon \{0,1\}^n \to \{+1,-1\}$. We use this version of the definition because it exactly captures the rank of the communication matrix for XOR functions (see Section A.1).

A.1 The approach of Lin and Zhang

We review the approach of Lin and Zhang [20] which we build upon in Section 4.2.

We first define the closure of min Certificate Complexity which was implicit in the approach of [35], and defined in [20]:

▶ **Definition A.5** (Closure of min Certificate Complexity; [35, 20]). *For a function $f\colon \{0,1\}^n \to \{0,1\}$, we define the closure of the min certificate complexity of f as:*

$$C^{clo}_{min}(f) = \max_{\alpha} C_{min}(f_\alpha)$$

where the maximum is taken over all possible partial assignments α on n variables, or in other words, over all possible subfunctions f_α of f.

Note that $C^{clo}_{min}(f) \leq C(f)$.

They also note that it is possible to define the closure for any complexity measure $M(f)$ for function f as $M^{clo}(f) = \max_\alpha M(f_\alpha)$, where the maximum is taken over all subfunctions f_α of f. A measure M is said to be downward non-increasing if for any function f, it holds that $M(f_\alpha) \leq M(f)$ for any subfunction f_α of f. Note that the measures sensitivity, block sensitivity, certificate complexity, decision tree complexity, $\mathbb{F}_2$-degree, Fourier sparsity, alternating number are all downward non-increasing. It follows from the definition of downward non-increasing measures that whenever measure M is downward non-increasing, it holds that $M^{clo}(f) = M(f)$.

We first note the following result from [7] stating that the rank of the communication matrix $M_{f\circ\oplus}$ exactly equals the Fourier sparsity of f:

▶ **Lemma A.6** ([7]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have: $rank(M_{f\circ\oplus}) = ||\hat{f}||_0$.*

Next, we note the following lemma about communication complexity of XOR functions:

▶ **Lemma A.7** ([25]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have: $CC(f \circ \oplus) \leq 2DT(f)$.*

The following lemma upper bounds the decision tree complexity in terms of the product of its certificate complexity and $\mathbb{F}_2$-degree. We note that the second inequality follows because $C^{clo}_{min}(f) \leq C(f)$.

▶ **Lemma A.8** ([36, 37, 20]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

$$DT(f) \leq C^{clo}_{min}(f) \cdot deg_2(f) \leq C(f) \cdot deg_2(f)$$

The $\mathbb{F}_2$-degree of any function is upper bounded by the logarithm of its Fourier sparsity as proved in [7]:

▶ **Lemma A.9** ([7]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have: $deg_2(f) \leq \log ||\hat{f}||_0$.*

Lemmas A.6, A.7, A.8, A.9 imply the following result as also noted in [20]:

▶ **Lemma A.10** ([20]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$:*

$$CC(f \circ \oplus) \leq 2C^{clo}_{min}(f) \cdot \log rank(M_{f\circ\oplus}) \leq 2C(f) \cdot \log rank(M_{f\circ\oplus})$$

It follows from Lemma A.10 that proving an upper bound on the certificate complexity of a function f in terms of a polynomial in $\log rank(M_{f\circ\oplus})$ would imply the log-rank conjecture for the corresponding XOR function $f \circ \oplus$.

Another approach towards proving the log-rank conjecture for XOR functions would be to upper bound $C^{clo}_{min}(f)$ directly. One way to achieve this for a class of functions would be to prove an upper bound of the form $C_{min}(f) \leq M(f)$ where $M(f)$ is a complexity measure that is downward non-increasing, since that would imply the bound $C^{clo}_{min}(f) \leq M(f)$, thereby proving the log-rank conjecture for functions $f \circ \oplus$ with bounded value of $M(f)$. Lin and Zhang [20] use this approach to prove that the log-rank conjecture holds for XOR functions $f \circ \oplus$ which are such that $alt(f)$ is at most polynomial in $\log ||\hat{f}||_0$.

In particular, they achieve this by proving that for every boolean function f, $C_{min}(f) \leq alt(f)deg_2(f)$. Since both $alt(f)$ and $deg_2(f)$ are downward non-increasing, they get the following result:

▶ **Theorem A.11** (Theorem 2 from [20]). *For any function $f\colon \{0,1\}^n \to \{0,1\}$, we have:*

$$CC(f \circ \oplus) \leq 2alt(f) \cdot \log^2 rank(M_{f\circ\oplus})$$

B Diameter under OR-composition

In this section, we study the behavior of diameters under OR-composition. In particular, we prove that any diameter of the OR-composition of two functions is upper bounded by a sum of their corresponding individual diameters (plus a constant factor).

In what follows, for two functions $f, g\colon \{0,1\}^n \to \{0,1\}$, we define the OR-composed function $f \vee g\colon \{0,1\}^{2n} \to \{0,1\}$ as $f \vee g(x_1, x_2) = 1$ if $f(x_1) = 1$ or $g(x_2) = 1$, and $f \vee g(x_1, x_2) = 0$ otherwise, for $x_1, x_2 \in \{0,1\}^n$.

We now prove a result relating the diameter of OR-composition of two functions with their individual diameters as mentioned before:

▶ **Theorem B.1.** *For any functions $f, g\colon \{0,1\}^n \to \{0,1\}$, we have:*

$$dia_\wedge(f \vee g) \leq dia_\wedge(f) + dia_\wedge(g) + 3$$

Proof. Consider any input $(x_1, x_2) \in \{0,1\}^{2n}$. We have two cases as follows:

Case 1: $f \vee g(x_1, x_2) = 0$. Consider the AND-NAND path $z_1^{(0)}, z_1^{(1)}, \ldots, z_1^{(t_1)}$ (where $\bar{x_1} = z_1^{(0)}$) achieving $dia_\wedge(f, x_1)$ and the AND-NAND path $z_2^{(0)}, z_2^{(1)}, \ldots, z_2^{(t_2)}$ (where $\bar{x_2} = z_2^{(0)}$) achieving $dia_\wedge(g, x_2)$.

We first deal with the case when $f(\bar{x_1}) = 0$ and $g(\bar{x_2}) = 0$. Observe that the following is a valid AND-NAND path for $f \vee g$:

$$(z_1^{(0)}, z_2^{(0)}), (z_1^{(0)}, z_2^{(1)}), \ldots (z_1^{(0)}, z_2^{(t_2)}), (z_1^{(1)}, z_2^{(t_2)}), (z_1^{(2)}, z_2^{(t_2)}), \ldots, (z_1^{(t_1)}, z_2^{(t_2)}).$$

This follows because of the simple observation, that for any input $(a, b) \in \{0,1\}^{2n}$, if $g(b) = 0$, then $f \vee g(a, b) = f(a)$. Due to this observation, in the first t_2 steps of the above path, the input to f is fixed to $z_1^{(0)}$ which is such that $f(z_1^{(0)}) = 0$. Therefore, throughout these steps, we have that $f \vee g(z_1^{(0)}, z_2^{(i)}) = g(z_2^{(i)})$ for any $i \in \{0, 1, \ldots t_2\}$. Since $z_2^{(0)}, z_2^{(1)}, \ldots, z_2^{(t_2)}$ is a valid AND-NAND path of g, the first t_2 steps form valid steps of an AND-NAND path of $f \vee g$.

Similarly, since $z_2^{(t_2)}$ agrees with a certificate for g on x_2, it holds that $g(z_2^{(t_2)}) = 0$. Therefore, for the next t_1 steps of the path, it holds that $f \vee g(z_1^{(i)}, z_2^{(t_2)}) = f(z_1^{(i)})$ for any $i \in \{0, 1, \ldots t_2\}$, and a similar argument goes through as for the first t_2 steps of the path.

Finally, since $z_1^{(t_1)}$ agrees with a certificate for f on x_1 and $z_2^{(t_2)}$ agrees with a certificate for g on x_2, the input $(z_1^{(t_1)}, z_2^{(t_2)})$ agrees on a certificate for $f \vee g$ on the input (x_1, x_2). We therefore get a valid AND-NAND path for the function $f \vee g$ of length $t_1 + t_2$.

Now, we consider the case when $f(\bar{x_1}) = 1$ and $g(\bar{x_2}) = 0$. In this case, we first perform an additional step of flipping the bits of any minimal sensitive block B for f on $\bar{x_1}$ to get to a 0-input of f i.e. $\bar{x_1}^B$. We then follow the argument of the previous case, and without changing the input to f, take t_2 steps corresponding to the AND-NAND path for g i.e. $z_2^{(0)}, z_2^{(1)}, \ldots, z_2^{(t_2)}$. We then "undo" the first step by flipping back the bits of B in the input corresponding to f to get to the input $(\bar{x_1}, z_2^{(t_2)})$. Finally, we take the t_1 steps of the AND-NAND path for f starting from input $\bar{x_1}$ to get a valid AND-NAND path of total length $t_1 + t_2 + 2$.

Similar argument works for the case when $f(\bar{x_1}) = 0$ and $g(\bar{x_2}) = 1$.

Finally, the case with $f(\bar{x_1}) = 1$ and $g(\bar{x_2}) = 1$ goes through a similar argument, with the difference that the first step involves simultaneously flipping minimal sensitive blocks for both f and g, on the respective inputs $\bar{x_1}$ and $\bar{x_2}$, to get input $(\bar{x_1}^{B_1}, \bar{x_2}^{B_2})$, say. The next step flips back these bits only for g to get the input $(\bar{x_1}^{B_1}, \bar{x_2})$. The argument then proceeds as in the previous case, where we take the AND-NAND path for g starting from input $\bar{x_2}$, followed by flipping back the bits of block B_1 for the input to f, followed by the AND-NAND path for f starting from input $\bar{x_1}$.

This gives a valid AND-NAND path of length $t_1 + t_2 + 3$ for $f \vee g$ starting from input $(\bar{x_1}, \bar{x_2})$.

Case 2: $f \vee g(x_1, x_2) = 1$. Wlog, assume that $g(x_2) = 1$.

In this case, we follow a similar proof strategy as in Case 1, with the difference that in this case, we only need to follow the steps corresponding to a valid AND-NAND path for g starting from $\bar{x_2}$, since in this case, a certificate for g on x_2 would also be a certificate for $f \vee g$ on (x_1, x_2). Apart from that, we follow a similar argument, where we first flip appropriate blocks of bits, if necessary, to ensure that we are at a 0-input of f. We then follow the AND-NAND path for g to get a certificate for $f \vee g$ on (x_1, x_2). This gives an AND-NAND path for $f \vee g$ of length at most $t_2 + 2$. ◀

We remark that Theorem B.1 also holds for the three other diameters we consider i.e. for $dia_{deg}(f)$, $dia_{deg_2}(f)$ and $dia_s(f)$ by an analogous argument.

Note that the TRIBES function $f\colon \{0,1\}^{n^2} \to \{0,1\}$ as discussed in Example 5.3 is an OR-composition of n copies of the AND_n function (i.e. the AND function on n bits). Since $dia_\wedge(AND_n) = 1$, Theorem B.1 implies the bound: $dia_\wedge(TRIBES) \leq \Theta(n)$. As seen in Example 5.3, $dia_\wedge(TRIBES) \geq 2n - 1$ and therefore, this bound is asymptotically tight for the TRIBES function.

However, Theorem B.1 does not always give a tight bound for OR-composed functions, as can be seen from the example of the function $OR_n\colon \{0,1\}^n \to \{0,1\}$ i.e. the OR function on n bits. OR_n is also an OR-composition of n copies of the function $g\colon \{0,1\} \to \{0,1\}$ with single-bit inputs, where $g(x) = x$. Since $dia_\wedge(g) = 1$, Theorem B.1 gives the bound $dia_\wedge(OR_n) \leq \Theta(n)$. This bound is not tight since it holds that $dia_\wedge(OR_n) = 1$.