# A note on the quasi-additive bound for Boolean functions

Kamiyama, Naoyuki



出版情報：Journal of Math-for-Industry (JMI). 4 (B), pp.119-122, 2012-10. Faculty of Mathematics, Kyushu University
バージョン：
権利関係：

Journal of Math-for-Industry, Vol. 4 (2012B-6), pp. 119–122

Math-for-industry
Education & Research Hub

# A note on the quasi-additive bound for Boolean functions

Naoyuki Kamiyama

Received on August 30, 2012 / Revised on September 13, 2012

**Abstract.** In this note, we prove that the linear programming for computing the quasi-additive bound of the formula size of a Boolean function presented by Ueno (2010) is equivalent to the dual problem of the linear programming relaxation of some integer programming for computing the protocol partition number.

*Keywords.* computational complexity, Boolean function complexity, protocol partition number

## 1. Introduction

Proving lower bounds for a concrete computational model is a fundamental problem in Computational Complexity [1]. In this note, we consider formula size lower bounds for a Boolean function. If we can show a super-polynomial formula size lower bound for a function in **NP**, it implies that $\mathbf{NC}^1 \neq \mathbf{NP}$ [10]. Karchmer and Wigderson [4] proved that the size of a smallest formula computing a Boolean function $f$ is equal to the protocol partition number of the communication matrix arising from $f$. Karchmer, Kushilevitz and Nisan [3] formulated the problem of computing a lower bound for a protocol partition number, called the rectangle bound, as an integer programming problem and introduced a technique which gives a lower bound by showing a feasible solution of the dual problem of its linear programming relaxation. It is known [8] that this technique subsumes techniques proposed in [5, 6, 7]. However, Karchmer, Kushilevitz and Nisan [3] also proved that this technique can not prove a lower bound larger than $4n^2$ for non-monotone formula size in general.

Recently, Ueno [11] introduced a novel technique, called the quasi-additive bound, which is inspired by the notion of subadditive rectangle measures presented by Hrubeš, Jukna, Kulikov and Pudlák [2]. Although the linear programming for computing the quasi-additive bound can be seen as a simple extension of the linear programming for computing the rectangle bound, Ueno [11] proved that the quasi-additive bound can surpass the rectangle bound and it is potentially strong enough to give the matching formula size lower bounds.

In this note, we prove that the linear programming for computing the quasi-additive bound of the formula size of a Boolean function $f$ presented by Ueno [11] is equivalent to the dual problem of the linear programming relaxation of some integer programming for computing the protocol partition number of the communication matrix arising from $f$. Together with the result of Ueno [11], our results imply that there exists no gap between our integer programming for computing the protocol partition number and its linear programming relaxation. We hope that the results of this note help to understand why the quasi-additive bound is more powerful than the rectangle bound. Furthermore, to the best of our knowledge, no one studied an exact integer programming formulation for computing a protocol partition number. Thus, it may be of independent interests.

## 2. Preliminaries

Let $\mathbb{R}$ and $\mathbb{Z}_+$ be the sets of reals and non-negative integers, respectively. Let $X$, $Y$ and $Z$ be finite sets. A non-empty subset of $X \times Y \times Z$ is called a **relation**. When we emphasize that a relation $T$ is a subset of $X \times Y \times Z$, then we say that $T$ is a relation on $(X, Y, Z)$. For each relation $T$ on $(X, Y, Z)$, define $C(T) := X \times Y$. We call an element of $C(T)$ a **cell**.

A **formula** is a binary tree with each leaf labeled by a literal and each non-leaf vertex labeled by either of the binary connectives $\vee$ and $\wedge$. A literal is either a variable or its negation. The size of a formula is defined by its number of literals. For a Boolean function $f$, we define formula size $L(f)$ as the size of a smallest formula computing $f$.

Karchmer and Wigderson [4] characterized the size of a smallest formula computing a Boolean function by using the notions of a communication matrix and a protocol partition number. Suppose that we are given a relation $T$ on $(X, Y, Z)$. The **communication matrix** $M(T)$ of $T$ is defined by a matrix whose rows and columns are indexed by $X$ and $Y$, respectively. Each cell $(x, y)$ of $C(T)$ contains elements $z$ of $Z$ such that $(x, y, z) \in T$. A non-empty direct product $X' \times Y' \subseteq X \times Y$ is called a **rectangle** of $M(T)$. We denote by $\mathcal{R}(T)$ the set of rectangles of $M(T)$. Define $\overline{\mathcal{R}}(T) := \mathcal{R}(T) \setminus \{X \times Y\}$. A rectangle $X' \times Y'$ is said to be **monochromatic**, if there exists an element $z$ of $Z$ such that $(x, y, z) \in T$ for every $(x, y) \in X' \times Y'$. Let $\mathcal{M}(T)$ be the set of monochromatic rectangles of $M(T)$. For a

$$
\begin{aligned}
\max \quad & \sum_{c\in C(T)} \phi(c) \\
\text{s.t.} \quad & \sum_{c\in R} \phi(c) + \sum_{c\in C(T)\setminus R} \psi(c,R) \le 1 \quad (\forall R \in \mathcal{M}(T)) \\
& \sum_{c\in C(T)\setminus V} \psi(c,V) + \sum_{c\in C(T)\setminus W} \psi(c,W) \ge \sum_{c\in C(T)\setminus R} \psi(c,R) \quad (\forall R \in \mathcal{R}(T),\ \forall \{V,W\} \in \mathcal{P}(R)) \\
& \phi \in \mathbb{R}^{C(T)},\ \psi \in \mathbb{R}^{C(T)\times \mathcal{R}(T)}
\end{aligned}
$$

Figure 1: A linear programming $\mathsf{QA}(T)$.

rectangle $X' \times Y'$, a **partition** of $X' \times Y'$ is defined by

- a pair of rectangles $X'_1 \times Y'$ and $X'_2 \times Y'$ such that $X' = X'_1 \cup X'_2$ and $X'_1 \cap X'_2 = \emptyset$, or
- a pair of rectangles $X' \times Y'_1$ and $X' \times Y'_2$ such that $Y' = Y'_1 \cup Y'_2$ and $Y'_1 \cap Y'_2 = \emptyset$.

We say that a set $\mathcal{R}$ of disjoint rectangles **recursively partitions** $M(T)$, if

$$\bigcup_{R\in\mathcal{R}} R = X \times Y.$$

and there exists a **rooted binary tree representation** of $\mathcal{R}$ defined as follows. A vertex of this tree corresponds to some rectangle of $M(T)$. Especially, the root vertex corresponds to $X\times Y$, and a leaf corresponds to a rectangle of $\mathcal{R}$. For each non-leaf vertex $v$, rectangles corresponding to its children consist of a partition of a rectangle corresponding to $v$. The size of a smallest set of disjoint monochromatic rectangles which recursively partitions $M(T)$ is called the **protocol partition number** of $M(T)$ and it is denoted by $C^P(T)$,

For each Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, define $f^{-1}(1)$ and $f^{-1}(0)$ by

$$
\begin{aligned}
f^{-1}(1) &:= \{x \in \{0,1\}^n \mid f(x) = 1\}, \\
f^{-1}(0) &:= \{x \in \{0,1\}^n \mid f(x) = 0\}.
\end{aligned}
$$

For each Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, define the relation $T_f$ by

$$T_f := \{(x,y,i) \in f^{-1}(1) \times f^{-1}(0) \times \{1,\dots,n\} \mid x_i \neq y_i\}.$$

Karchmer and Wigderson [4] gave the following characterization of the size of a smallest formula.

**Theorem 1** ([4]). *For each Boolean function $f$,*

$$C^P(T_f) = L(f).$$

### 2.1. Quasi-additive bound

Let $T$ be a relation on $(X,Y,Z)$. For each rectangle $R$ of $\mathcal{R}(T)$, let $\mathcal{P}(R)$ be the set of partitions of $R$. Now we consider the linear programming $\mathsf{QA}(T)$ described in Figure 1. Let $\mathsf{qa}(T)$ be the optimal objective value of an optimal solution for $\mathsf{QA}(T)$. The value $\mathsf{qa}(T)$ is called the **quasi-additive bound**. Although $\mathsf{QA}(T)$ can be seen as a simple extension of the linear programming for computing the rectangle bound (see [3]), Ueno [11] proved the following surprising result.

**Theorem 2** ([11]). *For each relation $T$,*

$$\mathsf{qa}(T) = C^P(T).$$

From Theorems 1 and 2, we can see the following corollary.

**Corollary 1** ([4, 11]). *For each Boolean function $f$,*

$$\mathsf{qa}(T_f) = L(f).$$

Let $\Gamma(T)$ be the set of ordered pairs $(R,P)$ of a rectangle $R$ of $\mathcal{R}(T)$ and a partition $P$ of $R$. Define the integer programming $\mathsf{PN}(T)$ as described in Figure 2. In $\mathsf{PN}(T)$, we use the notation $y(R,P)$ instead of $y((R,P))$. Let $\mathsf{LPN}(T)$ be the linear programming relaxation of $\mathsf{PN}(T)$. The following theorem was proved by Ueno [12].

**Theorem 3** ([12]). *For each relation $T$, $\mathsf{QA}(T)$ is equivalent to the dual problem of $\mathsf{LPN}(T)$.*

## 3. Main Results

Here we give our main result. For each relation $T$, let $\mathsf{pn}(T)$ be the objective value of an optimal solution of $\mathsf{PN}(T)$.

**Theorem 4.** *For each relation $T$,*

$$\mathsf{pn}(T) = C^P(T).$$

We will leave the proof of Theorem 4 to the next section. By Theorems 3 and 4, the following corollary can be obtained.

**Corollary 2.** *For each relation $T$, $\mathsf{QA}(T)$ is the dual problem of the linear relaxation of some integer programming for computing $C^P(T)$.*

Furthermore, by the weak duality theorem (see [9]) and Theorems 2, 3 and 4, the following corollary can be obtained. For each relation $T$, let $\mathsf{lpn}(T)$ be the objective value of an optimal solution of $\mathsf{LPN}(T)$.

**Corollary 3.** *For each relation $T$,*

$$\mathsf{pn}(T) = \mathsf{lpn}(T).$$

$$\begin{aligned}
\min \quad & \sum_{R \in \mathcal{M}(T)} x(R) \\
\text{s.t.} \quad & \sum_{R \in \mathcal{M}(T) \colon c \in R} x(R) = 1 \quad (\forall c \in C(T)) && (1) \\
& \sum_{(V,P) \in \Gamma(V) \colon R \in P} y(V,P) = \begin{cases} \sum_{P \in \mathcal{P}(R)} y(R,P) + x(R) & \text{if } R \in \mathcal{M}(T) \\ \sum_{P \in \mathcal{P}(R)} y(R,P) & \text{otherwise} \end{cases} \quad (\forall R \in \overline{\mathcal{R}}(T)) && (2) \\
& x \in \mathbb{Z}_+^{\mathcal{M}(T)}, \ y \in \mathbb{Z}_+^{\Gamma(T)}
\end{aligned}$$

Figure 2: An integer programming $\mathsf{PN}(T)$.

*Proof.* By Theorems 2, 3 and 4,

$$C^P(T) = \mathsf{qa}(T) \leq \mathsf{lpn}(T) \leq \mathsf{pn}(T) = C^P(T),$$

where the first inequality follows from the weak duality theorem. □

## 4. Proof

In this section, we give the proof of Theorem 4. Theorem 4 clearly follows from the following Lemmas 1 and 2.

**Lemma 1.** *Let $T$ be a relation, and let $\mathcal{M}'$ be a subsets of $\mathcal{M}(T)$ which recursively partitions $M(T)$. Define a vector $x \in \mathbb{Z}_+^{\mathcal{M}(T)}$ by*

$$x(R) := \begin{cases} 1, & R \in \mathcal{M}', \\ 0, & \text{otherwise.} \end{cases}$$

*Then, there exists $y \in \mathbb{Z}_+^{\Gamma(T)}$ such that $(x, y)$ is a feasible solution for $\mathsf{PN}(T)$.*

**Lemma 2.** *Let $T$ be a relation, and let $(x, y)$ a feasible solution for $\mathsf{PN}(T)$. Define*

$$\mathcal{M}_x := \{R \in \mathcal{M}(T) \mid x(R) = 1\}.$$

*Then, $\mathcal{M}_x$ recursively partitions $M(T)$.*

### 4.1. Proof of Lemma 1

Define $\mathcal{M}(T) := \mathcal{M}$, $\overline{\mathcal{R}}(T) := \overline{\mathcal{R}}$ and $\Gamma(T) := \Gamma$. Since (1) is clearly satisfied, it suffices to prove that (2) is satisfied.

Let $\mathcal{T}$ be a rooted binary tree representation of $\mathcal{M}'$. In the sequel, we do not distinguish between a vertex $v$ of $\mathcal{T}$ and the corresponding rectangle. Define a vector $y \in \mathbb{Z}_+^{\Gamma}$ as follows. If $R$ is a non-leaf vertex of $\mathcal{T}$ and the children of $R$ consist of a partition $P$, define $y(R, P) := 1$. Otherwise, define $y(R, P) := 0$. We will show that $(x, y)$ satisfies (2).

Let $R$ be a rectangle of $\overline{\mathcal{R}}$. We first assume that $R$ is is not contained in $\mathcal{T}$. In this case, $y(R, P) = 0$ for every partition $P$ of $R$ and $y(V, P) = 0$ for every $(V, P) \in \Gamma$ such that $R \in P$. Furthermore, if $R \in \mathcal{M}$, then $x(R) = 0$ follows from $R \notin \mathcal{M}'$. These imply that (2) satisfies.

Next we consider the case where $R$ is contained in $\mathcal{T}$. Since $R \neq X \times Y$, $R$ is not the root of $\mathcal{T}$. Hence, there exist the parent $W$ and the sibling $S$ of $R$ in $\mathcal{T}$. Define $Q := \{R, S\}$. Then, $y(W, Q) = 1$ and $y(V, P) = 0$ for every $(V, P) \in \Gamma$ such that $R \in P$ and $(V, P) \neq (W, Q)$. Thus, the left-hand side of (2) is equal to 1, and it suffices to show that the right-hand side of (2) is equal to 1.

If $R$ is a leaf of $\mathcal{T}$ (i.e., $R \in \mathcal{M}'$), then $x(R) = 1$ and $y(R, P) = 0$ for every partition $P$ of $R$. Thus, the right-hand side of (2) is equal to 1. If $R$ is a non-leaf vertex of $\mathcal{T}$, then $x(R) = 0$ by $R \notin \mathcal{M}'$. Let $Q'$ be a partition of $R$ which consist of the children of $R$ in $\mathcal{T}$. Then, $y(R, Q') = 1$ and $y(R, P) = 0$ for every partition $P$ of $\mathcal{P}(R)$ such that $P \neq Q'$. These facts imply that the right-hand side of (2) is equal to 1. This completes the proof.

### 4.2. Proof of Lemma 2

By (1), $\mathcal{M}_x$ partitions $M(T)$. So, what remains is to prove that it "recursively" partitions $M(T)$.

By induction on

$$\sum_{R \in \mathcal{M}(T)} x(R),$$

we prove the lemma. For every pair of a relation $T$ and a feasible solution $(x, y)$ for $\mathsf{PN}(T)$ such that

$$\sum_{R \in \mathcal{M}(T)} x(R) = 1,$$

we have $X \times Y \in \mathcal{M}(T)$ and $x(X \times Y) = 1$. So, the lemma clearly holds.

Assuming that the lemma holds for every pair of a relation $T$ and a feasible solution $(x, y)$ for $\mathsf{PN}(T)$ such that

$$\sum_{R \in \mathcal{M}(T)} x(R) = k \geq 1,$$

we consider a pair of a relation $T$ and a feasible solution $(x, y)$ for $\mathsf{PN}(T)$ such that

$$\sum_{R \in \mathcal{M}(T)} x(R) = k + 1.$$

We first prove the following claim.

**Claim 5.** *There exists* $(S, Q) \in \Gamma(T)$ *such that*

1. *both rectangles of* $Q$ *are monochromatic,*
2. $x(V) = 1$ *for both rectangles* $V$ *of* $Q$*, and*
3. $y(S, Q) > 0$.

*Proof.* Since

$$\sum_{R \in \mathcal{M}(T)} x(R) \geq 2,$$

there exists a rectangle $R$ of $\mathcal{M}(T)$ such that $x(R) = 1$ and $R \neq X \times Y$. Hence, by (2) there exists $(R, P) \in \Gamma(T)$ such that $y(R, P) > 0$. Let $(S, Q)$ be a pair of $\Gamma(T)$ such that $y(S, Q) > 0$ and $|S|$ is minimum. If $V$ is not monochromatic or $x(V) = 0$ for a rectangle $V$ of $Q$, it follows from (2) that $y(V, P) > 0$ for some $P \in \mathcal{P}(V)$, which contradicts $|S|$ is minimum. This completes the proof. □

Let $(S, Q)$ be a pair of $\Gamma(T)$ satisfying the conditions of Claim 5. Define $Q := \{V, W\}$. Since $V$ is monochromatic, there exists some element $z$ of $Z$ which every cell of $V$ contains. Here we consider a new relation $T'$ obtained from $T$ by adding $z$ to the entry of every cell of $W$. Define $x' \in \mathbb{Z}_+^{\mathcal{M}(T')}$ by

$$x'(R) := \begin{cases} 1, & \text{if } R = S, \\ 0, & \text{if } R = V \text{ or } R = W, \\ x(R), & \text{if } R \in \mathcal{M}(T) \text{ and } R \neq S, V, W, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, define $y \in \mathbb{Z}_+^{\Gamma(T')}$ by

$$y'(R, P) := \begin{cases} y(R, P) - 1, & \text{if } (R, P) = (S, Q), \\ y(R, P), & \text{otherwise.} \end{cases}$$

Notice that $y'(S, Q) \geq 0$ follows from $y(S, Q) > 0$. Since $S \notin \mathcal{M}(T)$ or $x(S) = 0$ by (1), we have

$$\sum_{R \in \mathcal{M}(T)} x(R) = k.$$

Hence, in order to use the induction hypothesis, we need the following claim.

**Claim 6.** $(x', y')$ *satisfies* (1) *and* (2) *for* $T'$.

*Proof.* Since (1) is satisfied by the definition of $x'$ and the induction hypothesis, we consider the constraint (2). By the definition of $(x', y')$ and induction hypothesis, it suffices to consider the constraint for $S$, $V$ and $W$.

First we consider the constraint for $S$. Since $x'(S) - x(S) = 1$ (if $S \notin \mathcal{M}(T)$, set $x(S) := 0$) and

$$\sum_{P \in \mathcal{P}(S)} y'(S, P) - \sum_{P \in \mathcal{P}(S)} y(S, P) = -1,$$

the right-hand side of (2) does not change. Hence, since the left-hand side does not change, (2) is satisfied. Next we consider the constraint for $V$. The left-hand side of (2) decreases by 1 due to $(S, Q)$. Since $x'(V) - x(V) = -1$, the right-hand side of (2) also decreases by 1. Hence, (2) is satisfies. The same argument is clearly valid for $W$. This completes the proof. □

By the induction hypothesis, $\mathcal{M}_{x'}$ recursively partitions $M(T')$. It is not difficult to see that we can construct a rooted binary tree representation of $\mathcal{M}_x$ by adding two vertices $V$ and $W$ under $S$ of the rooted binary tree representation of $\mathcal{M}_{x'}$. This completes the proof.

## References


[1] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[2] P. Hrubeš, S. Jukna, A. S. Kulikov, and P. Pudlák. On convex complexity measures. *Theor. Comput. Sci.*, 411(16-18):1842–1854, 2010.

[3] M. Karchmer, E. Kushilevitz, and N. Nisan. Fractional covers and communication complexity. *SIAM J. Discrete Math.*, 8(1):76–92, 1995.

[4] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3(2):255–265, 1990.

[5] V. M. Khrapchenko. Complexity of the realization of a linear function in the case of $\pi$-circuits. *Mathematical Notes*, 9:21–23, 1971.

[6] E. Koutsoupias. Improvements on Khrapchenko's theorem. *Theor. Comput. Sci.*, 116(2):399–403, 1993.

[7] S. Laplante, T. Lee, and M. Szegedy. The quantum adversary method and classical formula size lower bounds. *Computational Complexity*, 15(2):163–196, 2006.

[8] T. Lee. A new rank technique for formula size lower bounds. In *STACS'07*, volume 4393 of *LNCS*, pages 145–156, 2007.

[9] A. Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, 2003.

[10] P. Spira. On time-hardware complexity tradeoffs for boolean functions. In *4th Hawaii Symposium on System Sciences*, pages 525–527, 1971.

[11] K. Ueno. Breaking the rectangle bound barrier against formula size lower bounds. In *MFCS'10*, volume 6281 of *LNCS*, pages 665–676, 2010.

[12] K. Ueno. *Stronger LP Bounds for Formula Size Lower Bounds*. PhD thesis, The University of Tokyo, 2010.



Naoyuki Kamiyama
Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail: kamiyama(at)imi.kyushu-u.ac.jp