

Cohomology in Grothendieck Topologies and Lower Bounds in Boolean Complexity II: A Simple Example*

Joel Friedman[†]

March 31, 2006

Abstract

In a previous paper we have suggested a number of ideas to attack circuit size complexity with cohomology. As a simple example, we take circuits that can only compute the AND of two inputs, which essentially reduces to SET COVER. We show a very special case of the cohomological approach (one particular free category, using injective and skyscraper sheaves) gives the linear programming bound coming from the relaxation of the standard integer programming reformulation of SET COVER.

1 Introduction

In [Fri05] we introduced several techniques that may prove useful in using cohomology (on Grothendieck topologies) for obtaining lower bounds on circuit complexity. In this paper we simplify this problem to complexity involving only conjunctions of Boolean functions. We then show that a simple example of a Grothendieck topology, sheaves, and open sets lead to the “linear programming” bound. Furthermore we improve a bound in [Fri05].

*MSC 2000 classifications: primary: 68Q17, secondary: 14F20, 18G99

[†]Departments of Computer Science, University of British Columbia, Vancouver, BC V6T 1Z4, CANADA, and Departments of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, CANADA. jf@cs.ubc.ca, <http://www.math.ubc.ca/~jf>. Research supported in part by an NSERC grant.

Let S be a set, and denote by $\mathbb{B}^S = \{0, 1\}^S$ the collection of functions from S to $\mathbb{B} = \{0, 1\}$ (viewing 1 as TRUE and 0 as FALSE). By a *formal AND measure* we mean a function, h , from \mathbb{B}^S to the non-negative reals such that for all $f, g \in \mathbb{B}^S$ we have

$$h(f \wedge g) \leq h(f) + h(g)$$

(compare the notion of a *formal complexity measure*, e.g., see [Weg87]). Given a subset $\mathcal{S}_1 = \{f_1, \dots, f_r\}$, let $\text{size}(f)$ be the minimum number of elements of \mathcal{S}_1 whose conjunction is f ; we define $\text{size}(f)$ to be infinite if f cannot be expressed as such a conjunction. Equivalently $\text{size}(f)$ is the size of the smallest formula computing f via conjunctions of elements of \mathcal{S}_1 . By induction on “size” we see that for any formal AND measure, h , we have

$$\text{size}(f) \geq h(f)/M, \quad \text{where } M = \max_i h(f_i).$$

If h also satisfies

$$h(f) = h(\neg f),$$

then similarly we have an $h(f)/M$ lower bound on the size of a formula as before, but where the operations are either conjunctions or the negation of a conjunction; then $\log_2(h(f)/M)$ would bound the formula (or circuit) depth.

Given S and f_1, \dots, f_r , determining $\text{size}(f)$ is NP-complete. It can be approximated (to within $O(\log r)$) by a linear program. We shall show that the “virtual zero extensions” described in [Fri05], just in the special case of a free category with sheaves with no non-trivial higher cohomology, give this linear programming bound (or more precisely its dual). We finish by recalling the notion of virtual zero extensions.

We sketch the ideas, referring to [Fri05] for the details. Let \mathcal{C} be a finite category, and endow it with the *grosnière* topology (meaning that a sheaf is the same thing as a presheaf). Let F, G sheaves of finite dimensional \mathbb{Q} -vector spaces on \mathcal{C} , and let U be an open set of \mathcal{C} (i.e., a sieve), and Z be a closed set. We say that a sheaf, H , is a virtual $G_{U,Z}$ if there is an exact sequence,

$$0 \rightarrow G_U \rightarrow G_{U \cap Z} \oplus H \rightarrow G_Z \rightarrow 0,$$

where the maps $G_U \rightarrow G_{U \cap Z}$ and $G_{U \cap Z} \rightarrow G_Z$ are the usual maps (i.e., the identity on the intersection of the supports), and where G_A denotes G restricted to A and extended by zero outside A . See [Fri05] for conditions on the existence of H ; for a free category (see [Fri05]) H always exists. The following theorem is an improvement over the bound in [Fri05].

Theorem 1.1 *In the situation above, with H a virtual $G_{U,Z}$, we have*

$$\text{cc}(F, G_{U \cap \overline{Z}}) \leq \text{cc}(F, G) + \text{cc}(F, G_U) + \text{cc}(F, G_{\overline{Z}}),$$

where $\text{cc}(A, B)$ is the sum of the dimensions of $\text{Ext}_{\mathcal{C}}^i(A, B)$ over all non-negative i , and \overline{Z} is the complement of Z .

We shall prove this theorem in Section 3. Now assume that we have a map $f \mapsto U_f$ from \mathbb{B}^S to open sets of \mathcal{C} such that $U_{f \wedge g} = U_f \cap U_g$. Then

$$h(f) = \text{cc}(F, G_{U_f})$$

is a formal AND measure, provided that $\text{cc}(F, G) = 0$.

The idea to test the ideas of [Fri05] on AND's alone arose in conversations with Les Valiant. We wish to thank him, as well as Janos Simon, for discussions.

2 AND complexity

Given S and $\mathcal{S}_1 \subset \mathbb{B}^S$, determining $\text{size}(f)$ is NP-complete, as it is almost a reformulation of SET COVER (see [Vaz01], for example, for SET COVER); indeed, to determine how many \mathcal{S}_1 elements we need to obtain f , we may assume $f \leq f_i$ for all i , and then the question is how many $f_i^{-1}(0)$ are required to cover $f^{-1}(0)$. The point of this paper is to show that the dual of the usual “linear programming” lower bound on size/depth complexity arises as a very special (and degenerate) case of the sheaf bound. Specifically, the size complexity is given by the integer program

$$\begin{aligned} \min \sum_{i \in R} \mu_i, \quad & \text{subject to} \\ \sum_{i \in R} \mu_i (1 - f_i(s)) \geq 1, \quad & \forall s \in f^{-1}(0) \\ \mu_i = 0, 1 \quad & i \in R, \end{aligned}$$

where R is the set of i with $f \leq f_i$. A lower bound to this program is given by the “relaxed” linear program where the μ_i are non-negative reals. The gap between the integer and linear program is known to be as high as

$O(\log r)$ in certain cases, and never higher (see [Vaz01]). Equivalent to the linear program is its dual,

$$\begin{aligned} \max \quad & \sum_{s \in f^{-1}(0)} \alpha_s, & \text{subject to} \\ \sum_{s \in f^{-1}(0)} \alpha_s(1 - f_i(s)) & \leq 1, & \forall i \in R \\ \alpha_s & \geq 0 & \forall s \in S \end{aligned}$$

Say that $s \in f^{-1}(0)$ *demands* f_i if $f_i(s) = 0$ and $f_j(s) = 1$ for $j \neq i$. If for each $i = 1, \dots, r$ there is an s_i that demands f_i , then we take α_s to be 1 or 0 according to whether or not s is one of the s_i , and then we see that the LP-bound is exact, i.e., gives the true size complexity (namely r).

For example, consider the case where $S = \{0, 1\}^n$ and the size one functions are $\{0, 1, x_1, \neg x_1, \dots, \neg x_n\}$; given f , we discard 0, 1 and all size one functions not $\geq f$; we see that either f is the conjunction of the functions leftover, and the LP-bound is exact, or f is of infinite size complexity, and the LP-bound is also infinite (the primal is infeasible, and for the dual there is an s with $f(s) = 0$ but $f_i(s) = 1$ for all leftover f_i ; then α_s can be taken arbitrarily large).

3 Improved Inequality

In this section we prove Theorem 1.1.

The short exact sequence

$$0 \rightarrow G_{U \cap Z} \rightarrow G_U \xrightarrow{\beta} G_{U \cap Z} \rightarrow 0$$

gives a long exact sequence, yielding

$$\dim(\text{Ext}^i(F, G_{U \cap Z})) = \dim(\text{Coker } \beta^{i-1}) + \dim(\text{Ker } \beta^i), \quad (1)$$

where $\beta^i: \text{Ext}^i(F, G_U) \rightarrow \text{Ext}^i(F, G_{U \cap Z})$ are the maps arising from β . It suffices to bound the right-hand-side of equation (1).

The virtual zero extension gives a short sequence

$$0 \rightarrow G_U \xrightarrow{\beta \oplus \gamma} G_{U \cap Z} \oplus H \rightarrow G_Z \rightarrow 0.$$

Letting γ^i be, as before, the map γ in $\text{Ext}^i(F, \cdot)$ gives

$$\dim(\text{Ext}^i(F, G_Z)) = \dim(\text{Coker}(\beta^i \oplus \gamma^i)) + \dim(\text{Ker}(\beta^{i+1} \oplus \gamma^{i+1})).$$

Since $\text{Coker} \beta^i$ injects into $\text{Coker}(\beta^i \oplus \gamma^i)$, we have

$$\sum \dim(\text{Coker} \beta^i) \leq \sum \dim(\text{Coker}(\beta^i \oplus \gamma^i)) \leq \text{cc}(F, G_Z).$$

And clearly

$$\sum \dim(\text{Ker} \beta^i) \leq \sum \dim(\text{domain}(\beta^i)) = \sum \dim(\text{Ext}^i(F, G_U)) = \text{cc}(F, G_U).$$

Summing in equation (1) yields

$$\text{cc}(F, G_{U \cap \bar{Z}}) \leq \text{cc}(F, G_Z) + \text{cc}(F, G_U).$$

We now finish the proof using

$$\text{cc}(F, G_Z) \leq \text{cc}(F, G) + \text{cc}(F, G_{\bar{Z}})$$

that follows from the exact sequence

$$0 \rightarrow G_{\bar{Z}} \rightarrow G \rightarrow G_Z \rightarrow 0.$$

□

4 A Trivial Bound

In this section we use the notation of [Fri05]: if \mathcal{C} is a category and $P \in \text{Ob}(\mathcal{C})$, then k_P is the inclusion $\Delta_0 \rightarrow \mathcal{C}$ where Δ_0 is the category with one object, 0, and one morphism, and $k_P(0) = P$; also, if $u: \mathcal{C} \rightarrow \mathcal{C}'$ is a functor, u^* is the pullback and u_* (respectively $u_!$) is its right (respectively left) adjoint (this notation comes [sga72], Exposé I, Section 5.1).

Lemma 4.1 *Let \mathcal{C} be the free category on the graph, G . For a closed inclusion $i: Z \rightarrow \mathcal{C}$, let $\text{Hom}_Z(P, Q)$ be the set of all paths in G all of whose vertices except the last lie outside Z ; in particular, if $P \in Z$, then $\text{Hom}_Z(P, Q)$ is empty if $Q \neq P$ and consists of a single element (the zero length path about P) if $Q = P$. For any $P \in \text{Ob}(\mathcal{C})$ we have that*

$$i_* i^* k_{P*} \mathbb{Q} \simeq \bigoplus_{Q \in Z} (k_{Q*} \mathbb{Q})^{\text{Hom}_Z(P, Q)}. \quad (2)$$

Proof Let F_L, F_R denote the sheaves on the left- and right-hand-side of equation (2). First note that i_*i^* is simply restriction to Z followed by extension by 0, and F_R clearly vanishes outside Z . So it suffices to give an isomorphism $F_L(X) \simeq F_R(X)$ for each $X \in Z$ that is functorial in X .

We have that $(k_{P*}\mathbb{Q})(X)$ is $\text{Hom}(P, X)$ copies of \mathbb{Q} , and $\text{Hom}(P, X)$ is the number of paths in G from P to X . For each path in G from P to X , once a vertex in the path, Q , falls in Z , all subsequent vertices remain in Z . Hence we have a set theoretic bijection

$$b_X: \bigcup_Q \text{Hom}_Z(P, Q) \times \text{Hom}(Q, X) \rightarrow \text{Hom}(P, X)$$

for each X . Furthermore this bijection is functorial in X , in that if $\phi: X_1 \rightarrow X_2$ is a morphism, then we have that $\phi b_{X_1} = b_{X_2} \phi$, the second ϕ acting on each $\text{Hom}(Q, X_1)$. This gives the desired functorial isomorphism $F_L(X) \simeq F_R(X)$.

□

Now let S be a finite set, and let M_S be the graph whose vertices are the functions $S \rightarrow \{0, 1\}$ with one or zero edges from f to g according to whether or not $f \leq g$ and $f(s) = g(s)$ for all but exactly one $s \in S$. Let \mathcal{C} be the free graph on M_S . We call M_S the *monotone S -cube*, and \mathcal{C} the *S -path category*. For $f \in \text{Ob}(\mathcal{C})$, let U_f be the smallest open set containing f , i.e., the set of all objects no greater than f . By a *subcube* of \mathcal{C} we mean a collection of objects whose values at a subset of S are fixed.

Consider the model, $f \mapsto (\mathcal{C}, F, G_{U_f})$, where $G = k_{P*}\mathbb{Q}$ and where F and P are to be specified later. Since \mathcal{C} is free, virtual zero extensions always exist. If Z_f denotes the complement of U_f , we have

$$\text{cc}(f) = \sum_{Q \in Z_f} (\dim F(Q)) |\text{Hom}_{Z_f}(P, Q)|.$$

Of course, the $\dim F(Q)$ can be arbitrary non-negative integers by taking F to be a sum of skyscraper sheaves, i.e., a sheaf, F , where for each morphism $\phi \in \mathcal{C}$ we have $F\phi$ is the zero morphism.

We claim this recovers the linear programming bound. Indeed, let $P = 0$, and let F vanish outside of the points δ_s where $s \in S$ and δ_s is the Dirac delta function at s . Then $\text{cc}(F, G) = 0$, since $F(0) = 0$, and

$$\text{cc}(g) = \sum_s A_s(1 - g(s)),$$

where A_s is the dimension of $F(\delta_s)$. So we get

$$\text{size}(f) \geq \sum_s A_s/M,$$

for any M with

$$\sum_s A_s(1 - f_i(s)) \leq M;$$

this is just the linear programming bound (restricted to $\alpha_s = A_s/M$ rational, α_s as in Section 2). Furthermore, it is not hard to see that varying G injective and F arbitrary and taking linear combinations we cannot get anything better than the linear programming bound. Indeed, since $f = 0$, we have $\text{cc}(f) = 0$ unless $P = 0$; so any $P \neq 0$ terms can be discarded in an optimal bound. Similarly, if $P = Q$, then $\text{cc}(F, G)$ is already 1 and $\text{cc}(f)$ is no greater, so such terms can be discarded (since the bound $\text{size}(f) \geq 1$ can always be achieved by the linear program). Finally, if $P = 0$ and $Q \neq 0$ and $Q \neq \delta_S$, then

$$\text{cc}(f) = \sum_{(A,B) \in E_S} N_{P,Q}(A, B) \text{cc}_{A,B}(f),$$

where E_S are the edges of G_S , $N_{P,Q}(A, B)$ is the number of paths from P to Q in G_S that pass through the edge (A, B) , and $\text{cc}_{A,B}$ denotes the cohomological complexity when $P = A$ and F is zero outside B and \mathbb{Q} on B . In the above displayed sum we may discard the A with $A \neq 0$, as mentioned before, and we are left with a cohomological complexity as before.

The bound we get on $\text{size}(f)$ can, of course, be derived without cohomology. Indeed, consider any formal function

$$h(f) = \sum_{\phi \in \text{Hom}_{Z_f}(P, \cdot)} A(\phi), \tag{3}$$

where A is a any non-negative function. Then h is a formal AND measure, since $\text{Hom}_{Z_{f \wedge g}} \subset \text{Hom}_{Z_f} \cup \text{Hom}_{Z_g}$.

We pause for a mild generalization of this notion. By a *conjunctively closed family* we mean an $C \subset \mathbb{B}^S$ such that $f, g \in C$ implies $f \wedge g \in C$; by a *conjunctively closed complement* we mean the complement in \mathbb{B}^S of a conjunctively closed family, or equivalently a $B \subset \mathbb{B}^S$ such that $f \wedge g \in B$ implies at least one of f, g lies in B . For such a B , we have χ_B , the characteristic function of B is a formal AND measure, and therefore so is

any non-negative linear combination of such characteristic functions; this is an essential generalization of the h in equation (3).

Let us mention that taking $G = (k_{P*}\mathbb{Q})_U$ for an open set, U , yields such a bound; indeed, it is not hard to see that we get $\text{cc}(f)$ as in equation (3) with $A(\phi) = \beta(t\phi)$ with

$$\beta(Q) = \dim F(Q) + \dim V(Q) - 2 \text{rank}(M),$$

where

$$V(Q) = \bigoplus_{\chi \in \text{Hom}_{\overline{\mathbb{F}}}(Q, \cdot)} F(t\chi),$$

and $M: V(Q) \rightarrow F(Q)$ is the map whose χ component is $F(\chi)$; clearly β (and therefore A) is non-negative.

References

- [Fri05] Joel Friedman. Cohomology of grothendieck topologies and lower bounds in boolean complexity. 2005. <http://www.math.ubc.ca/~jf>, also <http://arxiv.org/abs/cs/0512008>, to appear.
- [sga72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos.* Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, Vol. 269.
- [Vaz01] Vijay V. Vazirani. *Approximation algorithms.* Springer-Verlag, Berlin, 2001.
- [Weg87] Ingo Wegener. *The complexity of Boolean functions.* Wiley-Teubner Series in Computer Science. John Wiley & Sons Ltd., Chichester, 1987.