ISSN 0105-8517

# A measure in which Boolean negation is exponentially powerful

Sven Skyum

DAIMI PB-154
September 1982

Computer Science Department
**AARHUS UNIVERSITY**
Ny Munkegade – DK 8000 Aarhus C – DENMARK
*Telephone: 06 – 12 83 55*

A measure in which Boolean negation
is exponentially powerful

by
Sven Skyum

## 1. Introduction

One of the intriguing questions in combinatorial complexity theory is the power of negation. Pippenger [3] has shown that for almost all monotone Boolean functions $f_n$ in n variables, $C_{B_2}(f_n) = \Theta(2^n/n^{3/2})$ where $B_2$ is the set of all 16 two-argument functions and $C_B(f)$ is the size of the smallest circuit representing f using operations from B. Following Lubanov [2] we get that for all monotone Boolean functions $f_n$, $C_{\{\wedge,\vee\}}(f_n) = O(2^n/n)$ so for most monotone Boolean functions $f_n$ only a factor of order $\sqrt{n}$ in circuitsize can be gained by allowing negation. No family of functions has yet been found where either formula- or circuitsize has been less by more than a constant factor by allowing negation.

A question in the same line has been considered by Bloniarz and Meyer (see [1]) who show that there exist monotone Boolean functions $f_n$ in n variables such that $L_{B_2}(f_n) = O(n)$ and $L_{\{\vee,\wedge\}}(f_n) = \Theta(n^2)$ where $L_B(f)$ is the formulasize over B of f.

This latter result does not indicate the power of negation since $L_{\{\vee,\wedge,\neg\}}(f_n) = \Theta(n^2)$ It rather indicates the power of $\oplus$ (exclusive or).

In this paper we demonstrate that for more restricted representations negation can be exponentially powerful. The representation uses the notions of projections and universality from [5] and the result shows that nonmonotone projections can be exponentially more powerful than monotone ones. This solves one of the problems left open in [5].

## 2. Notations and definitions

We will use the three operations $\vee$ (OR), $\wedge$ (AND) and $\neg$ (NEGATION). $\neg x$ will be written as $\bar{x}$. 0 and 1 will represent FALSE and TRUE.

A formula is defined inductively as follows:
(a) 0 and 1 are formulae, (b) $x$ and $\bar{x}$ are formulae if $x$ is a variable, and (c) $(F_1)\vee(F_2)$ and $(F_1)\wedge(F_2)$ are formulae if $F_1$ and $F_2$ are formulae. We omit redundant parentheses.

A formula F represents in the usual way a (Boolean) function. The size $L(F)$ of a formula F is the number of occurrences of 0, 1, $x_i$ and $\bar{x}_i$ (for all i) in F. The formulasize $L(f)$ of a function f is $\min\{L(F) \mid F \text{ represents } f\}$.

The function $f(\underline{x})$ is monotone iff for all $j\in\{1,..,n\}$ and $b_1,\ldots,b_n\in\{0,1\}$, $f(b_1,\ldots,b_{j-1},0,b_{j+1},\ldots,b_n) = 1 \Rightarrow f(b_1,\ldots,b_{j-1},1,b_{j+1},\ldots,b_n) = 1$.

The function $f(x_1,\ldots,x_n)$ is a projection of $g(y_1,\ldots,y_m)$ if there is a mapping $\sigma\colon \{y_1,\ldots,y_m\} \to \{0,1,x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ such that $f(x_1,\ldots,x_n) = g(\sigma(y_1),\ldots,\sigma(y_m))$. The projection is monotone if $\sigma\colon \{y_1,\ldots,y_m\} \to \{0,1,x_1,\ldots,x_n\}$.

A family P of functions is a sequence $\{P_n\}_{n\in S}$ where $P_n$ is a function of n variables and $S\subseteq\mathbb{N}$.

A family P is (monotone) universal if all (monotone) functions f are (monotone) projections of some members of P.



The (monotone) representation size with respect to a (monotone) universal family P for a (monotone) function f is defined to be the smallest m such that f is a (monotone) projection of $P_m$. We denote the measure $P(f)$ $(P_+(f))$.

Example

Let DNF be given by

$$DNF_{n^2}(\underline{x}) = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{n} x_{ij} \,.$$

Since all functions can be represented by a formula in disjunctive normal form, we have that DNF is (monotone) universal. We can furthermore note that for all monotone functions f, $DNF(f) = DNF_+(f)$ so negation does not help with respect to DNF.

Let $\underline{x} = \{x_{ij} \mid 1\le i<j\le n\}$ be $n(n-1)/2$ Boolean variables. We consider $\underline{x}$ as an $n\times n$ adjacency matrix for an undirected graph $G[\underline{x}]$ with n vertices $\{1,2,\ldots,n\}$ and edges $\{i,j\}$ according to the values of $x_{ij}$. We can denote an edge $\{i,j\}$ by $\{i,j\}$:1 and no edge by $\{i,j\}$:0. Since all our graphs will be undirected we will just write "graph" and assume that it is undirected. Let $v(\underline{x})$ denote the number of vertices, n, of $G[\underline{x}]$.

## 3. The connectivity problem

In [5] it is shown that similar looking families can give substantially different monotone measures. If we define s-t connectedness STCON as

$$STCON_{n(n-1)/2}(\underline{x}) = \begin{cases} 1 & \text{if two designated vertices s and t in } G[\underline{x}] \text{ are connected.} \\ 0 & \text{otherwise} \end{cases}$$

and connectedness CON as

$$CON_{n(n-1)/2}(\underline{x}) = \begin{cases} 1 & \text{if } G[\underline{x}] \text{ is connected} \\ 0 & \text{otherwise} \end{cases}$$

then for all f, $STCON_+(f) \le 2L(f)^2$ while there exist infinitely many g such that $CON_+(g) \ge 2^{L(g)-1} - 3\cdot 2^{L(g)/2}$.

The family used in [5] to demonstrate the exponential lower bound was

$$g_{2n}(\underline{x}) = (x_1 \wedge x_2) \vee (x_3 \wedge x_4) \vee \ldots \vee (x_{2n-1} \wedge x_{2n}).$$

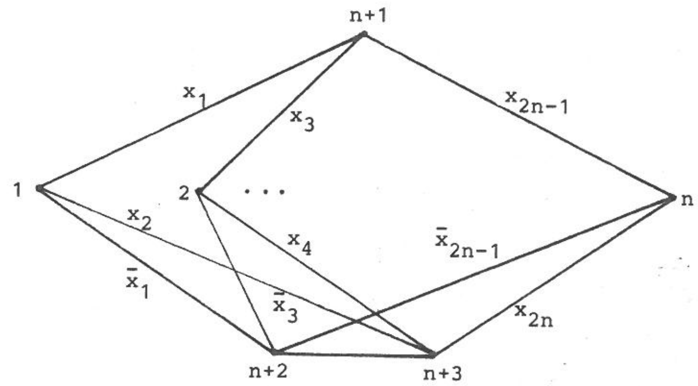
It was shown that if $g_{2n}(\underline{x}) = CON_{m(m-1)/2}(\sigma(\underline{y}))$ where $\sigma$ is a monotone projection then $2^n - 1 \le m \le \sqrt{n}(2^n-1)$.

CON is not useful to project from with respect to monotone projections because of the exponential lower bound. If we on the other hand allow negation, the picture changes drastically as Theorem 1 demonstrates. Before stating the theorem we introduce the technique by proving that $g_{2n}(\underline{x}) = CON_{m(m-1)/2}(\sigma(\underline{y}))$ for some $\sigma$ and m=n+3.

Let m=n+3 and define $\sigma$: $\{y_{ij}\} \to \{0,1,x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ as follows:

$$\begin{aligned} \sigma(y_{i,n+1}) &= x_{2i-1} && \text{for } 1 \le i \le n, \\ \sigma(y_{i,n+2}) &= \bar{x}_{2i-1} && \text{for } 1 \le i \le n, \\ \sigma(y_{i,n+3}) &= x_{2i} && \text{for } 1 \le i \le n, \\ \sigma(y_{n+2,n+3}) &= 1 && \text{and} \\ \sigma(y_{ij}) &= 0 && \text{otherwise.} \end{aligned}$$






$G[\sigma(\underline{y})]$

Figure 1

$\sigma$ is defined such that the vertices 1 to n are connected to either vertex n+1 or vertices n+2 and n+3 in $G[\sigma(\underline{y})]$. Thus $CON_{m(m-1)/2}(\sigma(\underline{y})) = 1$ iff $G[\sigma(\underline{y})]$ is connected iff $x_{2i-1} = x_{2i} = 1$ for some i iff $g_{2n}(\underline{x}) = 1$.

The following Theorem shows that this construction can be generalized to obtain a much stronger result.

**Theorem 1**

For all Boolean functions f,

$$CON(f) \le L(f)^{\alpha} \quad \text{for} \quad \alpha = 2\log_2 3.$$

Before proving the Theorem we need two Lemmas. The first is a technical one to be used in the evaluation of $\alpha$.

Lemma 1

For $\beta = \log_2 3$ we have for $1 \leq a \leq b$ $(a+b)^\beta \geq 2a^\beta + b^\beta$.

Proof

It suffices to prove that for $x \geq 1$

$$F(x) = (1+x)^\beta - x^\beta - 2 \geq 0.$$

This holds because it holds for x=1 and the derivative $F'(x) = \beta(1+x)^{\beta-1} - x^{\beta-1}$ is greater than or equal to 0 if $x \geq 1$. ∎

The second one is about transforming arbitrary formulae into formulae which are suited for our construction. We say that a formula F is suitable iff it is the case that if $F_1 \wedge F_2$ is a subformula of F then $F_1 \vee F_2$ describes the constant function 1.

Lemma 2

If f is a Boolean function then there is a suitable formula for f of size at most $L(f)^\beta$ where $\beta = \log_2 3$.

Proof

Assume $f = f_1 \wedge f_2$ and $F_1, F_2, F_1'$ and $F_2'$ are suitable formulae for $f_1$, $f_2$, $\bar{f}_1$ and $\bar{f}_2$. Then $F = F_1 \wedge (F_1' \vee F_2)$ and $F' = F_1' \vee F_2'$ are suitable formulae for f and $\bar{f}$. Similarly if $f = f_1 \vee f_2$ then $F = F_1 \vee F_2$ and $F' = F_1' \wedge (F_1 \vee F_2')$ are suitable formulae for f and $\bar{f}$. Let $m(f) = \max\{L(F), L(F')\}$. If we always choose $f_1$ and $f_2$ such that $m(f_1) \leq m(f_2)$ then we get that for $f = f_1 \wedge f_2$ or $f = f_1 \vee f_2$, $m(f) \leq 2m(f_1) + m(f_2)$. Combining this with Lemma 1 and $m(x) = m(\bar{x}) = m(0) = m(1) = 1$ we get the result. ∎



Proof of Theorem 1

Let $f(\underline{x})$ be an arbitrary Boolean function in n variables and let F be a minimal suitable formula describing it. We will prove by induction in L(F) that we can define a projection $\sigma: \{y_{12}, y_{13}, \ldots, y_{m-1,m}\} \to \{0, 1, x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ such that

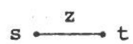
(1) $m \leq L(F)+1$,

(2) There are two designated vertices s and t in $G[\sigma(\underline{y})]$ such that all nodes in $G[\sigma(\underline{y})]$ are connected to either s or t.

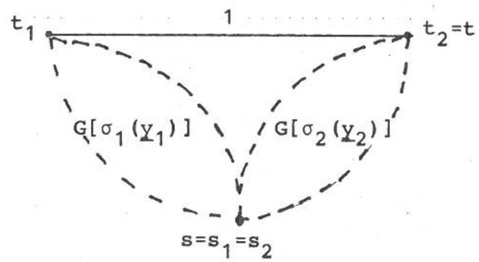
(3) $f(\underline{x}) = CON_{m(m-1)/2}(\sigma(\underline{y}))$.

The construction is analogous to the construction in [5] but only works for suitable formulae.

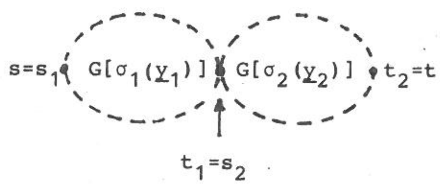
(i) If F=z (z=0, 1, x or $\bar{x}$) then define $\sigma$ such that $G[\sigma(\underline{y})]$ is




(ii) If $F = F_1 \vee F_2$ then $G[\sigma(\underline{y})]$ should be




(iii) If $F = F_1 \wedge F_2$ then $G[\sigma(\underline{y})]$ should be



In (ii) and (iii) $\sigma_i$: $\{\underline{y}_i\} \to \{0,1,x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ with $m_i = v(\underline{y}_i)$ is assumed to satisfy (1) to (3) with respect to $F_i$ and $f_i$ where $F_i$ represents $f_i$.

Let v be an arbitrary vertex in $G[\sigma_1(\underline{y}_1)]$ say (the case where v is in $G[\sigma_2(\underline{y}_2)]$ is similar). Then by assumption v is either connected to $s_1$ or $t_1$. If $F=F_1 \vee F_2$ then it is immediate that v is connected to s or t since they are connected to $s_1$ and $t_1$ respectively. If $F=F_1 \wedge F_2$ and v is connected to $s_1$ it is connected to s (= $s_1$) by definition. Now assume that v is not connected to $s_1$ but to $t_1$. Then $f_1=0$ since $G[\sigma_1(\underline{y}_1)]$ is disconnected, but then $f_2=1$ since F is suitable so $t_1=s_2$ and v are connected to t (= $t_2$). Since (2) is obviously true for f=z we have proven (2). Having (2), (3) becomes easy and is left to the reader together with (1).

Altogether we get that $CON(f) \le m(m-1)/2$ for $m \le L(F)+1 \le L(f)^{\beta}+1$ which implies that $CON(f) \le [L(f)^{2\beta}+L(f)^{\beta}]/2+1 \le L(f)^{\alpha}$ where $\beta = \log_3 2 = \alpha/2$. ∎



Acknowledgment

I want to thank Dexter Kozen for helpful comments and suggestions on a first draft of this paper.

References

[1] : Bloniarz, P.A.: The complexity of monotone Boolean functions and an algorithm for finding shortest paths in a graph. Ph.D. Thesis, MIT/LCS/TR-238.

[2] : Lupanov, O.B.: Ob odnom metode sinteza skhem. Izv. V.U.Z. Radiofiz 1 (1958) pp. 120-140.

[3] : Pippenger, N.: The complexity of monotone Boolean functions. Math. System Theory 11 (1978) pp. 289-316.

[4] : Savage, J.E.: The complexity of computing. Wiley (1974).

[5] : Skyum, S. and Valiant, L.G.: A complexity theory based on Boolean algebra. Proc. 22nd ann. IEEE FOCS (1981) pp. 244-253.

[6] : Valiant, L.G.: Completeness classes in algebra. Proc. 8th ACM STOC (1979) pp. 249-261.