A Note on Nečiporuk's Method for Nondeterministic Branching Programs

Paul Beame Pierre McKenzie

August 16, 2011

Abstract

Nečiporuk [Neč66] gave a method based on counting subfunctions to lower bound the formula size over an arbitrary binary basis and contact scheme (or Boolean branching program) size required to compute explicit n-input Boolean functions. Pudlak [Pud87] observed that Nečiporuk's method also yields an $\Omega(n^{3/2}/\log n)$ lower bound on switching-and-rectifier network size as well as *nondeterministic* branching program size [Raz91], and Karchmer and Wigderson [KW93] extended this lower bound to apply to span program size.

In this note, we show that any lower bound achievable by Nečiporuk's method is at most $O(n^{3/2}/\log n)$ for any of these three models. As part of our argument we show that every n-input Boolean function can be computed by a nondeterministic branching program of size $O(2^{n/2})$ and this is asymptotically optimal.

1 Introduction

Relatively few methods exist to prove complexity lower bounds in general non-uniform models of computation. Among these, the method introduced by Nečiporuk [Neč66] method still yields the best lower bounds known today for explicit functions in a number of complexity measures. Nečiporuk's method may be applied to any complexity measure for which (1) the overall cost can be allocated to individual input variables, (2) the assignment of a value to any input variable cannot increase the contribution of the other variables to the total cost of the resulting restricted function, and (3) the number of functions of low complexity can be bounded.

In particular, there are explicit functions for which Nečiporuk's method yields lower bounds of $\Omega(n^2/\log n)$ on formula size over an arbitrary basis, $\Omega(n^2/\log^2 n)$ on deterministic branching program size and on contact

scheme size, and $\Omega(n^{3/2}/\log n)$ on nondeterministic branching program size, switching-and-rectifier network size, and span program size. All of these are the best known lower bounds for these complexity measures for any explicit function. The first two of these lower bounds are contained in Nečiporuk's original paper [Neč66]. Pudlak [Pud87] showed that Nečiporuk's method yields the third lower bound for switching-and-rectifier network size as well as for *nondeterministic* branching program size [Raz91], and Karchmer and Wigderson [KW93] showed that it also applies to span program size.

Nečiporuk's method yields a large lower bound for a function f if there is a partition of the input variables of f so that for many of the blocks in this partition there are many different subfunctions of f that can be derived by assigning values to variables outside that block. For example, two simple explicit functions that yield the lower bounds mentioned above are the Element Distinctness function and the Indirect Storage Access function. It is natural to try to optimize the use of this method, both in terms of how the bound depends on the numbers of subfunctions for each block in the partition and whether there are other choices of function for which one can prove stronger lower bounds.

For formula size over arbitrary bases, it is well known (see, e.g., [Weg87, Sav76]) that $\Theta(n^2/\log n)$ is indeed the best lower bound obtainable by Nečiporuk's method. Savage [Sav76] also cites Paterson (unpublished) as improving the constant factor in the bound. Similarly, $\Theta(n^2/\log^2 n)$ is the best lower bound obtainable by Nečiporuk's method for deterministic branching program size, as noted by Wegener [Weg87, p. 422], who states the claim with a hint at its proof. Moreover, Alon and Zwick [AZ89] derived the optimal multiplicative constant in this lower bound as a function of the number of subfunctions of f in each block.

Since the first two bounds using Nečiporuk's method are asymptotically the best possible it is natural to ask whether the third lower bound also uses Nečiporuk's method in an optimal way. Jukna seems to be the only one who has explicitly addressed this question. In his discussion [Juk01, p. 207] of the $\Omega(n^{3/2}/\log n)$ lower bound on span program size due to Karchmer and Wigderson [KW93] and based on Nečiporuk's method, he states that the method "cannot lead to much larger lower bounds" but does not give more details. In this note we give a more precise result, namely that the best bound on nondeterministic branching program size obtainable by Nečiporuk's method is indeed $\Theta(n^{3/2}/\log n)$. This automatically applies to span program size and switching-and-rectifier network size since these measures are upper-bounded by nondeterministic branching program size.

In deriving lower bounds using Nečiporuk's method, the major difference

between measures is the bound in part (3) above on the number of functions of low complexity with respect to each measure. In most presentations of Nečiporuk's method, such as those in [Weg87, BS90, Weg00], this bound is determined *syntactically*, for example, via a count of the number of syntactically distinct formulas of a given size or of syntactically distinct branching programs with a given number of nodes. However, this is an overcount of the number of different functions since, for example, many syntactically distinct branching programs may compute the same function. If only *semantically* distinct objects are counted, one may, in principle, obtain stronger lower bounds using Nečiporuk's method. In the case of deterministic branching programs, Alon and Zwick [AZ89] considered the stronger semantic version of Nečiporuk's bound and showed nonetheless that both semantic and syntactic versions reach the same asymptotic limit.

Our argument on the limitations of Nečiporuk's method for nondeterministic branching programs applies to its semantic version as well as its syntactic version. To do this we must lower bound the number of semantically distinct functions of small nondeterministic branching program size. We do this by showing that every n-input Boolean function can be computed by a nondeterministic branching program of size $O(2^{n/2})$. The large number of such functions yields the bound we seek. We also show that this size bound is asymptotically optimal – most n-input Boolean functions require nondeterministic branching program size $\Theta(2^{n/2})$. This shows that the so-called "Shannon effect" [Weg87] – that typical functions have asymptotically maximal complexity – also holds for nondeterministic branching programs (though our upper and lower bounds differ by a constant factor).

2 Definitions and Background

We begin by defining nondeterministic branching programs.

Definition A Boolean nondeterministic branching program (NBP) P on $\{0,1\}^n$ is a directed (loopless) multi-graph with a single start node s and a single sink node t of out-degree 0. Each non-sink node is labeled by a variable x_i for some $i \in [n]$. Each directed edges is labeled 0 or 1. For each assignment $a \in \{0,1\}^n$, the subgraph $P[a]$ of P consists of those edges e of P such that the source of e is labeled by a variable x_i such that the label of e is a_i. The Boolean function computed by P is 1 if and only if there is an st-path in $P[a]$. The *size* of P is the number of non-sink nodes in P.

We also mention the definition of switching-and-rectifier (RS) networks in passing. Their definition is related but somewhat different from NBPs – their graphs are undirected and edges either have labels that are literals or are unlabeled with a similar acceptance condition to NBPs. The size of an RS network is the number of its labeled edges. One can easily simulate Boolean NBPs by RS networks of at most twice the size – each NBP node becomes an RS node with two labeled children which have unlabeled edges to the corresponding destination nodes in the NBP. Span programs are even more powerful than RS networks but we omit their definition.

Definition Let $N(n,s)$ be the number of syntactically distinct n-input Boolean NBPs of size at most s. Let $N_{sem}(n,s) \leq N(n,s)$ be the number of distinct functions computed by n-input Boolean NBPs of size at most s.

Definition Let $f : \{0,1\}^n \to \{0,1\}$. For $V \subseteq [n]$, define $r_V(f)$ to be the number of *sub-functions of f on V*; i.e., the number of $g : \{0,1\}^V \to \{0,1\}$ such that there is some partial assignment ρ on $[n] \backslash V$ such that $g(y) = f|_\rho(y)$ for all $y \in \{0,1\}^V$.

Proposition 2.1. *For any $f : \{0,1\}^n \to \{0,1\}$ and $V \subseteq [n]$, $r_V(f) \leq \min\{2^{2^{|V|}}, 2^{n-|V|}\}$.*

Proof. $r_V(f)$ is at most the number of Boolean functions on V and at most the number of partial assignments to $[n] \setminus V$. □

Nečiporuk's lower bound method as applied to NBPs computing an n-input Boolean function f is given by the following:

1. For suitable values of $v \leq n$, compute upper bounds on the number of distinct NBPs, $u(v,s) \geq N_{sem}(v,s)$ of size at most s on $v \leq s$ variables.
2. Choose a partition $V_1, \ldots, V_p$ of $[n]$.
3. For each i, compute a lower bound $\ell_{V_i}(f) \leq r_{V_i}(f)$.
4. Conclude that $NBP(f) \geq 1 + \sum_{i \in [p]} s_i$ where $s_i = \min\{s \mid u(|V_i|, s) \geq \ell_{V_i}(f)\}$ since the number of NBP nodes with labels in V_i must be large enough to compute all possible subfunctions of f that are induced by fixing the variables in $[n] \setminus V$.

Proposition 2.2. $N_{sem}(n,s) \leq N(n,s) \leq n^s 2^{2s^2}$.

Proof. There are n choices for the node labels and at most 2^s possible node subsets for destinations of the out-edges labeled each of 0 and 1. □

Corollary 2.3. *For any $\epsilon > 0$, at least a $1-o(1)$ fraction of n-input Boolean functions have NBP size at least $(1-\epsilon)\cdot 2^{n/2}/\sqrt{2}$.*

Proof. There are 2^{2^n} Boolean functions on n inputs. For $s = 2^{n/2}/2$, we have $N_{sem}(n,s) \le n^s 2^{2s^2} \le 2^{2^{n/2}\log_2 n/\sqrt{2}} 2^{(1-\epsilon)^2 2^n}$ which is $o(2^{2^n})$. □

Proposition 2.4. *For any partition $V_1, \ldots, V_p$ of $[n]$,*

$$NBP(f) \ge 1 + \sum_{i=1}^{p} \sqrt{\log_2 r_{V_i}(f)/3}.$$

Proof. For $|V_i| \le s$, by Proposition 2.2 $N_{sem}(|V_i|,s) \le N(|V_i|,s) \le |V_i|^s 2^{2s^2} \le s^s 2^{2s^2}$. We compute s_i in the Nečiporuk outline as a function of $r_{V_i}(f)$ In particular for $N_{sem}(|V_i|,s) \ge r_{V_i}(f)$, we must have $2^{3s^2} \ge s^s 2^{2s^2} \ge r_{V_i}(f)$ and hence $s_i \ge \sqrt{\log_2 r_{V_i}(f)/3}$. □

Two natural functions for which Nečiporuk's method have yielded the asymptotically strongest results known so far are the Element Distinctness function and the Indirect Storage Access function. The Element Distinctness function ED_n is defined on $n = 2k2^k$ bits viewed as $m = 2^k$ integers in the range $[m^2]$ and and equal to 1 iff these integers all have different values. The Indirect Storage Access function $ISA_{k,\ell}$ is defined on $n = k + 2^k\ell + 2^\ell$ bits which are viewed as a k-bit index vector a, a sequence of 2^k ℓ-bit registers $x_0, \ldots, x_{2^k-1}$, and 2^ℓ 1-bit memory cells $y_0, \ldots, y_{2^\ell-1}$. The output of $ISA_{k,\ell}$ is y_{x_a}.

Proposition 2.5. *$NBP(ED_n)$ and $NBP(ISA_{k,\ell})$ for $\ell = k + \lceil \log_2 k \rceil$ are both $\Omega(n^{3/2}/\log n)$.*

Proof. The following argument for ED_n also appears as [BS90, Thm. 6.5] and is credited there to the first author and Cook. In the case of ED_n, the $m = 2^k$ blocks in the partition are the $2k$ bits corresponding to each integer. For each such block V_i, there is a different function resulting from each subset of $m-1$ other distinct integers in $[m^2]$; hence $r_{V_i}(ED_n) \ge \binom{m^2}{m-1} \ge m^{m-1}$ and $\sqrt{\log_2 r_{V_i}(ED_n)}$ is $\Omega(\sqrt{m \log m})$. There are m such blocks to the lower bound is $\Omega(m^{3/2}\log^{1/2} m)$ which is $\Omega(n^{3/2}/\log n)$.

In the case of $ISA_{k,\ell}$, the blocks in the partition that contribute to the lower bound are the sets V_i consisting of each of the 2^k ℓ-bit registers x_i.

For such a block V_i, only consider assignments to the remaining variables such that $a = i$. In this case, each y vector of 2^ℓ bits induces a different function of the V_i bits so $r_{V_i}(ISA_{k,\ell}) \geq 2^{2^\ell}$. Hence $\sqrt{\log_2 r_{V_i}(ISA_{k,\ell})} \geq 2^{\ell/2}$. There are 2^k such blocks and hence the lower bound is at least $2^k 2^{\ell/2}$. Since $\ell = k + \lceil \log_2 k \rceil$ and $n = k + 2^k \ell + 2^\ell$, 2^ℓ is $\Theta(n)$ and 2^k is $\Theta(n/\log n)$ and the hence the lower bound is $\Theta(n^{3/2}/\log_2 n)$. □

3 Upper bounds on NBP size and the power of Nečiporuk's method for NBPs

Lemma 3.1. *Every n-input Boolean function can be computed by an oblivious NBP of size at most $3 \cdot 2^{\lceil n/2 \rceil}$ and depth n.*

Proof. Assume that $n = 2t$ is even. The constructed NBPs will have only one nondeterministic level, will be the same for all functions for the other levels 1 to $t-1$ and $t+1$ to $2t$, and every node at each level i will query variable x_i.

The first $t-1$ levels form a compete decision tree of height $t-1$ on variables $x_1, \ldots, x_{t-1}$ with a node at level t for each assignment $a_1 \ldots a_{t-1}$ to these variables. The last t levels of the NBP consist of a complete fan-in tree of height t on variables $x_{t+1}, \ldots, x_{2t}$ as follows: There is a node at level $t' > t$ for every assignment $a_{t'} \ldots a_{2t}$ to $x_{t'} \ldots x_t$ and there is an out-edge labeled $a_{t'}$ from this node to the node at level $t'+1$ corresponding to $a_{t'+1} \ldots a_{2t}$. The 1-output node has two in-edges, one labeled a_{2t} from each node a_{2t} at level $2t$.

Finally, we define the nondeterministic level t of the NBP for function f. For each assignment $a_1, \ldots, a_{2t}$ on which f evaluates to 1, there is an out-edge labeled a_t from node corresponding to $a_1 \ldots a_{t-1}$ at level t (which queries x_t) to the node corresponding to $a_{t+1} \ldots a_{2t}$ at level $t+1$.

The constructed NBP has at most $3 \cdot 2^t = 3 \cdot 2^{n/2}$ nodes. □

Corollary 3.2. *For $n \geq 2\lfloor \log_2(s/3) \rfloor$, $N_{sem}(n,s) > 2^{s^2/36}$.*

Proof. Clearly $N_{sem}(n,s)$ is non-decreasing in n, so it suffices to prove the corollary for $n = 2\lfloor \log_2(s/3) \rfloor$. Then $3 \cdot 2^{n/2} \leq s < 6 \cdot 2^{n/2}$. There are precisely $2^{2^n} > 2^{s^2/36}$ different Boolean functions on n inputs and, by Lemma 3.1, each may be computed by an NBP of size at most s. □

This bound, together with Proposition 2.2, shows that the numbers of semantically distinct and syntactically distinct nondeterministic branching programs of a given size are polynomially-related to each other.

Theorem 3.3. *The largest lower bound on NBP size for computing n-input Boolean functions that may be obtained by Nečiporuk's method is $\Theta(n^{3/2}/\log n)$.*

Proof. Let f be an n-input Boolean function. By Corollary 3.2, in applying Nečiporuk's method to f, for any block V_i in the partition with $|V_i| \geq 2\lfloor \log_2(s/3) \rfloor$, $N_{sem}(|V_i|, s) > 2^{s^2/36}$. Now s_i is at least the minimum s such that $N_{sem}(|V_i|, s) \geq r_{V_i}(f)$, which is no larger than the minimum s such that $2^{s^2/36} \geq r_{V_i}(f)$ and $|V_i| \geq 2\lfloor \log_2(s/3) \rfloor$, Hence the contribution s_i of the block V_i to the lower bound is at most $\lceil 6\sqrt{\log_2 r_{V_i}(f)} \rceil$ for $|V_i|$ at least $\log_2 \log_2 r_{V_i}(f) + 2$. The only case that remains to analyze is when $|V_i| < \log_2 \log_2 r_{V_i}(f) + 2$. In this case, we use Lemma 3.1 to say that s_i is at most $3 \cdot 2^{\lceil |V_i|/2 \rceil}$ which is at most $6\sqrt{2 \log_2 r_{V_i}(f)}$.

This implies that, up to a small constant factor, Proposition 2.4 yields the asymptotically optimal lower bound possible for NBPs using Nečiporuk's method. It remains to show that for any n-input Boolean function f and every input partition the lower bound derived using Proposition 2.4 for f using that partition is $O(n^{3/2}/\log n)$.

Now by Proposition 2.1, $r_{V_i}(f) \leq \min\{2^{2^{|V_i|}}, 2^{n-|V_i|}\}$. Letting $v_i = |V_i|$, up to a constant factor, we have that the Nečiporuk lower bound for NBPs for any function is at most

$$\begin{aligned}
&\max\{\sum_i \sqrt{\log_2 \min\{2^{2^{v_i}}, 2^{n-v_i}\}} \mid \sum_i v_i = n\} \\
&= \max\{\sum_i \sqrt{\min\{2^{v_i}, n - v_i\}} \mid \sum_i v_i = n\} \\
&= \max\{\sum_i b(v_i) \mid \sum_i v_i = n\}.
\end{aligned}$$

where $b(v) = \min\{2^{v/2}, \sqrt{n - v}\}$.

Clearly, $b(v) = 2^{v/2}$ for $v \leq \log_2 n - 1$ and hence $b(v) + b(v') \leq b(v + v')$ if $v + v' \leq \log_2 n - 1$. It follows that without loss of generality we can assume that at most one v_i is smaller than $(\log_2 n - 1)/2$. Such a small v_i has $b(v_i) = 2^{v_i/2} < n^{1/4}$. There are at most $2n/(\log_2 n - 1)$ larger v_i with $v_i \geq (\log_2 n - 1)/2$, and each has $b(v_i) \leq \sqrt{n - v_i} \leq \sqrt{n}$. Hence $\sum_i b(v_i) \leq 2n^{3/2}/(\log_2 n - 1) + n^{1/4}$ which completes the proof. □

4 Final notes

We did not seriously try to optimize the constant factor in our bounds. The constant factor difference between the upper and lower bounds for

Nečiporuk's method for NBPs is in part due to the gap between the upper and lower bounds for the worst-case NBP size of n-bit Boolean functions.

Klauck [Kla07] has shown how the ideas used in Nečiporuk's bound can be extended to randomized formula size and quantum formula size, as well as formula size for nondeterministic formulas with limited nondeterminism. He observed that the logarithm of the number of distinct subfunctions of a function f on a given block V_i of variables is precisely the one-way two-player communication complexity of computing f with one player, who holds the portion of the input outside of V_i and can send a single message to the other player, who holds the part of the input in V_i and must compute the value of f. He derived lower bounds for randomized, quantum, and nondeterministic formulas by considering the same one-way communication problems for randomized, quantum, and nondeterministic communication complexity with limited nondeterminism. He also showed that, up to constant factors, the Nečiporuk-style lower bounds for computing total functions by ordinary formulas also apply to randomized and quantum formulas and hence $\Theta(n^2/\log n)$ bounds are also the best possible. It remains however to determine the best possible Nečiporuk-style lower bound achievable for nondeterministic formulas with limited nondeterminism.

References

[AZ89] N. Alon and U. Zwick. On Nečiporuk's theorem for branching programs. *Theor. Comput. Sci.*, 64(3):331–342, 1989.

[BS90] R. B. Boppana and M. Sipser. The complexity of finite functions. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume A, pages 757–804. Elsevier, 1990.

[Juk01] S. Jukna. *Extremal combinatorics - with applications in computer science*. Springer, 2001.

[Kla07] Hartmut Klauck. One-way communication complexity and the Nečiporuk lower bound on formula size. *SIAM J. Comput.*, 37(2):552–583, 2007.

[KW93] M. Karchmer and A. Wigderson. On span programs. In *Proceedings 8th Structure in Complexity Theory*, pages 102–111. IEEE Computer Society Press, 1993.

[Neč66] È. Nečiporuk. On a boolean function. *Doklady of the Academy of the USSR*, 169(4):765–766, 1966. English translation in *Soviet Mathematics Doklady* 7:4, pp. 999-1000.

[Pud87] P. Pudlák. The hierarchy of boolean circuits. *Computers and artificial intelligence*, 6(5):449–468, 1987.

[Raz91] A. Razborov. Lower bounds for deterministic and nondeterministic branching programs. In *8th Internat. Symp. on Fundamentals of Computation Theory*, pages 47–60, 1991.

[Sav76] J. E. Savage. *The Complexity of Computing.* John Wily, New York, 1976.

[Weg87] I. Wegener. *The Complexity of Boolean Functions.* Wiley-Teubner series in computer science. B. G. Teubner & John Wiley, Stuttgart, 1987.

[Weg00] I. Wegener. *Branching Programs and Binary Decision Diagrams.* SIAM Monographs on Discrete Mathematics and Applications. Soc. for Industrial and Applied Mathematics, Philadelphia, 2000.