A note on read-once branching programs for blocking sets in projective planes

S. Jukna*
Dept. of Computer Science
University of Trier
D-54286 Trier, Germany

A. Razborov†
Steklov Mathematical Institute
Vavilova 42, 117966, GSP–1
Moscow, Russia

November 25, 1996

Abstract

We exhibit a simple Boolean function f in n variables such that *both* the function f and its negation $\neg f$ have *nondeterministic* read-once branching programs of size $n^{5/2}$ but f requires *deterministic* read-once branching programs of size $2^{\sqrt{n}}$. This means that $\mathrm{P} \neq \mathrm{NP} \cap co - \mathrm{NP}$ in the context of read-once branching programs.

Let $P = \{1, \ldots, n\}$ be the set of points of a projective plane $\mathrm{PG}(2, q)$ of order q, and let $L_1, \ldots, L_n$ be the lines, viewed as subsets of P; hence $n = q^2 + q + 1$. Recall that each line has exactly $q + 1$ points; every two lines intersect in exactly one point and exactly $q + 1$ lines meet in one point. A *blocking set* is a set of points which intersects every line. The smallest blocking sets are just the lines. Blocking sets containing a line are called *trivial*.

The first function in AC^0 (*Exact-Perfect-Matching*) that requires exponential size read-once branching programs was exhibited in [4]. Gál in [3] showed that one can use for this purpose the characteristic function

$$g(x_1, \ldots, x_n) \rightleftharpoons \bigwedge_{i=1}^{n} \bigvee_{j \in L_i} x_j$$

of all blocking sets in $\mathrm{PG}(2, q)$ by proving that it has no deterministic read-once branching program of size smaller than $2^{\sqrt{n}}$. In this note we observe that, using known lower bounds on the size of blocking sets due to Bruen [2] and Blokhuis [1], the argument of [3] can be easily modified to get another result, namely that $\mathrm{P} \neq \mathrm{NP} \cap co - \mathrm{NP}$ in the context of read-once branching programs.

*Supported by DFG grant Me 1077/10–1. On leave from Institute of Mathematics, Vilnius, Lithuania.
E-mail: jukna@ti.uni-trier.de

†Supported by grant # 96-01-01222 of the Russian Basic Research Foundation.
E-mail: razborov@class.mi.ras.ru

We consider the usual model of *branching programs* (b.p.) (see e.g. [7, 5]). The program is *read-once* if on each path every variable is tested at most once. We use abbreviations 1-b.p. and 1-n.b.p. for deterministic and non-deterministic read-once branching programs.

Consider the function

$$f(x_1,\ldots,x_n) \rightleftharpoons g(x_1,\ldots,x_n) \wedge \neg T^n_{q+k+1}(x_1,\ldots,x_n),$$

where $k=(q+1)/2$ if q is a prime, and $k=\sqrt{q}$ otherwise; $T^n_s(x_1,\ldots,x_n)$ is the usual threshold function which outputs 1 iff $x_1+\ldots+x_n \geq s$. Thus, for any input $a: P \to \{0,1\}$, $f(a)=1$ iff the set $a^{-1}(1)$ is blocking and has at most $q+k$ points. This modified function has the required property:

> *Both f and $\neg f$ have 1-n.b.p. of size $n^{5/2}$ whereas any 1-b.p. computing f must have size exponential in k.*

Upper bound. Associate with each of n lines L_i $(i=1,\ldots,n)$ the following two Boolean functions. Assume for simplicity that $L_i=\{1,\ldots,q+1\}$. Then define $\varphi_i \rightleftharpoons x_1 \wedge \ldots \wedge x_{q+1} \wedge \neg T^n_k(x_{q+2},\ldots,x_n)$ and $\psi_i \rightleftharpoons \neg x_1 \wedge \ldots \wedge \neg x_{q+1}$.

Bruen in [2] proved that any non-trivial blocking set in a projective plane of order q must have at least $q+\sqrt{q}+1$ points, and this lower bound is known to be tight when q is a square. For the prime order q, Blokhuis [1] improved Bruen's bound to $3(q+1)/2$ (which is also optimal). By these bounds we have that $f(a)=1$ iff a has at most $q+k$ ones and contains some line L, i.e., $a(i)=1$ for all points $i \in L$. Thus, f is an OR of n functions $\varphi_1,\ldots,\varphi_n$, each of which has a 1-b.p. of size $n^{3/2}$. Hence, f has a 1-n.b.p. of size $n^{5/2}$. On the other hand, $\neg f(a)=1$ iff either a has more than $q+k$ ones or a avoids some line (or both). Thus, $\neg f$ is also an OR of the threshold function T^n_{q+k+1} and n functions $\psi_1,\ldots,\psi_n$, each of which has a 1-b.p of size $q+1$. Hence, f has a 1-n.b.p. of size $O(n^{3/2})$.

Lower bound. It is a 'folklore observation' (see [4], Lemma 4.1; or [3] for a simple proof) that any 1-b.p. computing a Boolean function f must have size at least 2^k-1 if f is *k-mixed* in the following sense: for any subset of points $I \subseteq P$ with $|I|=k$, and any two different assignments $a,b: I \to \{0,1\}$, there is an assignment $c: P \setminus I \to \{0,1\}$ for which $f(a,c) \neq f(b,c)$.

It is therefore enough to verify that our concrete function f is k-mixed. To show this, let I,a,b be as above and take an $i \in I$ for which $a(i)=1$ and $b(i)=0$. There are $q+1$ lines containing the point i. Since $|I-\{i\}|=k-1 \leq q-1$ (the number of lines containing i, minus two) we can find among them two lines L_1 and L_2 such that $L_1 \cap I = L_2 \cap I = \{i\}$. Define the assignment $c: P \setminus I \to \{0,1\}$ by letting $c(j)=1$ iff $j \in L_1$. Then inputs (a,c) and (b,c) both have at most $|I \cup L_1| \leq q+k$ ones. Thus, $f(a,c)=1$ since (a,c) contains the line L_1, which in turn, intersects all other lines. On the other hand, $f(b,c)=0$ since (b,c) does not intersect the line L_2, because $L_2 \cap (I \cup L_1)=\{i\}$ and $b(i)=0$. ∎

There is another simple way to generate examples separating $\mathrm{NP} \cap co-\mathrm{NP}$ from P in the context of read-once b.p. Let $n=2^l$ and $m=n/l$ be integers. Every Boolean function τ on m variables induces the following *pointer* function $f_\tau(X)$ in n variables $X=\{x_1,\ldots,x_n\}$. Divide X into l subsequent blocks $X_1,\ldots,X_l$ with m variables in

each, and define $f_\tau(X)$ to be the value of the j-th variable in the i-th block, where i and j are defined by the equality: $(i-1)m + j = \tau(X_1) + 2\tau(X_2) + \cdots + 2^{l-1}\tau(X_l)$.

Observe that if τ has a 1-b.p. of size ℓ then *both* f_τ and $\neg f_\tau$ have 1-n.b.p. of size $O(n\ell)$. The desired 1-n.b.p. first guesses a pair (i, j), after which it remains to test if the j-th variable in the i-th block has the value 1 (or 0 in the case of $\neg f_\tau$), and if the values $\tau(X_1), \ldots, \tau(X_l)$ coincide with the corresponding bits in the binary representation of (fixed at this point) integer $(i-1)m + j$.

For the function f_τ to be k-mixed it is enough that τ has the following property: $(*)$ no assignment of constants to k variables makes τ a constant function. This property ensures that, for any two different assigments a and b of constants to the same set of k variables in X, the rest can be arranged so that the string $\tau(X_1), \ldots, \tau(X_l)$ points to a bit where a and b differe. Thus, f_τ is k-mixed.

For example, if $s < m/2$ then the threshold function $\tau = T_s^m$ has the property $(*)$ with $k = s - 2$, and hence, the resulting function f_τ requires 1-b.p. of size exponential in $\Omega(m) = \Omega(n/\log n)$. This example appeared in ([4], Example 6.14). Since threshold function is not in AC^0, the resulting function f_τ is also outside this class. Savický [6] observed that, in fact, one can take simpler function τ: split the variables into $s = \sqrt{m}$ blocks of equal size, and let τ be the OR of ANDs of variables in these blocks. This function still has the property $(*)$ with $k = s - 1$, and the resulting function f_τ belongs to AC^0.

We conclude with one open problem. Interesting aspect of Bruen-Blokhuis function is that – unlike for pointer-like functions f_τ – the 1-n.b.p. for both f and $\neg f$ have extremely transparent structure, similar to that of the *disjunctive normal form*. Does there exists a function such that both it and its negation have disjunctive normal forms of polynomial size, but whose 1-b.p. (or at least the *decision tree*) size is exponential?

Acknowledgment

We would like to thank Petr Savický for his remarks on the preliminary version of this note. The first author would also like to thank Aart Blokhuis for interesting discussion about the structure of blocking sets (not reflected in this note).

References

[1] A. Blokhuis (1994) On the size of a blocking set in PG$(2, p)$. *Combinatorica* **14** 111–114.

[2] A. A. Bruen (1970) Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.* **76** 342-344.

[3] A. Gál (1995) A simple function that requires exponential size read-once branching programs. Tech. Rep. TR-95-09, University of Chicago, (submitted to *IPL*).

[4] S. Jukna (1988) Entropy of contact circuits and lower bounds on their complexity, *Theor. Comput. Sci.* **57** 113–129.

[5] A. A. Razborov (1991) Lower bounds for deterministic and nondeterministic branching programs. *Proc. FCT'91*, Lecture Notes in Computer Science **529** (Springer, Berlin) 47-60.

[6] P. Savický (1996) *Personal communication.*

[7] I. Wegener (1987) *The complexity of Boolean functions*, Wiley-Teubner.