Matrix Rank Arguments for Proving Lower Bounds on the Size of Branching Programs *

Christoph Meinel
FB IV - Informatik, Universität Trier
D-54286 Trier
meinel@uni-trier.de

Stephan Waack
Inst. für Num. u. Angew. Mathematik,
Georg-August-Universität
D-37083 Göttingen
waack@namu01.gwdg.de

Introduction

In order to characterize and investigate different logarithmic space–bounded complexity classes like $\mathcal{L}$, $\mathcal{NL}$, co$\mathcal{NL}$, $\oplus\mathcal{L}$, or $\mathcal{MOD}_p\mathcal{L}$ by means of combinatorial computational devices, *branching programs* [Lee59], Ω*-branching programs*, $\Omega \subseteq \mathbb{B}_2$ [Mei89] (this model includes the nondeterministic and co–nondeterministic branching programs), and MOD_p*-branching programs* [DKMW94] were introduced and investigated. Unfortunately, up to now, it was impossible to prove a superpolynomial lower bound on the size of any of these devices which would be a prerequiste for separating the corresponding complexity classes. In order to get a better understanding of the difficulties in deriving such lower bounds, certain restricted branching program models like *ordered binary decision diagrams* (OBDD's) or *oblivious linear length branching programs* were considered.

Based on results of [AM86, KMW89, Kra90, DKMW94], we have developed a theory of communication within deterministic, nondeterministic, co-nondeterministic, parity and MOD_p–branching programs. The restriction the considered branching

*Proc. of the Workshop on *Algebraic Methods in Complexity Theory*, Madras, 5–21, 1994

programs are supposed to fulfill is the *bounded alternating* property: A branching program P with this property is characterized by the fact that there are two disjoint subsets Y, $Z \subseteq X$ in the set X of variables tested in P, $\#Y = \#Z = \Theta(\#X)$, such that, on each path of P, the number of alternations between testing variables from Y and testing variables from Z is bounded by $(\#X)^{o(1)}$. With algebraical rank arguments concerning certain communication matrices, we are able to derive exponential lower bounds on the sizes of all the mentioned types of bounded alternating branching programs.

Bounded alternating branching programs provide a quite natural and general type of branching programs. For example, ordered binary decision diagrams (OBDD's) are bounded alternating. More interesting, due to a Ramsey theoretic lemma of Alon and Maass [AM86], the well investigated oblivious branching programs of linear length [AM86, KMW89, Kra90, DKMW94] are bounded alternating. However, we could show that bounded alternating branching programs are strictly more powerful than oblivious linear length-bounded ones. The investigation of bounded alternating branching programs also generalizes the settings of classical communication complexity theory in at least two important aspects. On one hand, it ignores a considerable portion of the input variables (the set $X - (Y \cup Z)$ of size $O(\#X)$) on which no is posed. On the other hand, it does not preassume the sets Y and Z. Hence, the complexity of bounded alternating branching programs reflects in a certain sense the amount of communication with respect to any disjoint subsets (of a partition) of the input.

This paper is structured as follows:

In Section 1, the algebraically based concept of ω-branching programs, ω: $I\!N \longrightarrow \mathcal{R}$, semiring homomorphism onto a finite semiring $\mathcal{R}$, is introduced which provides a general framework for analysing communication complexity aspects in the theory of branching programs. In Section 2, the model of bounded alternating ω-branching programs is introduced. In Section 3 a lower bound technique for bounded alternating ω-branching programs is presented that is mainly based on algebraical rank considerations of certain communication matrices. Then, in Section 4, we derive some exponential lower bounds on the $\mathcal{R}$-ranks of certain communication matrices that seem to be interesting not only in the context of branching programs. By means of the results of Sections 3 and 4, in Section 5, we derive some exponential lower bounds on the size of bounded alternating ω-branching programs. Finally, in Section 6, we summarize our results as separations of complexity classes related to bounded alternating ω-branching programs.

Full proofs and additional material can be found in the journal version of [MW93].

1 ω–Branching Programs

Let $\mathcal{R} = [\mathcal{R}; +_{\mathcal{R}}, 0_{\mathcal{R}}, \cdot_{\mathcal{R}}, 1_{\mathcal{R}}]$ be a finite semiring with a null element $0_{\mathcal{R}}$ and a one element $1_{\mathcal{R}}$, and let ω, $\omega : \mathbb{N} \longrightarrow \mathcal{R}$, be a semiring homomorphism from $\mathbb{N} = [\mathbb{N}; +, 0, \cdot, 1]$ onto $\mathcal{R}$. (Obviously, ω is uniquely determined.)

An ω–*branching program* P is a directed acyclic graph where each node has outdegree $\leq \#\mathcal{R}$. There is a distinguished node v_s, the *source*, which has indegree 0. Exactly two nodes, v_0 and v_1, are of outdegree 0. They are called *0-sink* and *1-sink* of P, respectively. Nodes of outdegree $\#\mathcal{R}$ are labeled with variables x over $\mathcal{R}$, $x \in X = \{x_1, \ldots, x_n\}$, or remain unlabeled as the remaining nodes of P. Each edge starting in a labelled node is labeled with an element r, $r \in \mathcal{R}$, such that no two edges starting in one node have the same label.

Each input $a = a_1 \ldots a_n \in \mathcal{R}^n$ defines some *computational paths* in P: Starting at the source v_s, a node v of P is connected with one of its successor nodes. If v is labeled with the variable x_i, then v is connected with the successor node of v which is reached from v via the edge labeled with a_i. A computational path is said to be *accepting* if it ends up in the 1-sink v_1. The number of accepting computational paths is denoted by $acc_P(a)$, $acc_P(a) \in \mathbb{N}$. Now, P is said to *accept* $a \in \mathcal{R}^n$ iff $\omega(acc_p(a)) = 1_{\mathcal{R}}$.

Obviously, ω-branching programs generalize teh concept of ordinary branching programs where each non-sink node is assumed to be labeled with a Boolean variable. Hence, for each input, there is exactly one computational path which is accepting if it ends up in the 1-sink.

Moreover, ω-branching programs generalize Ω-branching programs introduced in [Mei89], $\Omega \subseteq \mathbb{B}_2$, and MOD_p-branching programs introduced in [DKMW94], $p \in \mathbb{N}$. In order to see this consider the following semirings and semiring homomorphisms

$$\omega_{\vee} : \mathbb{N} \longrightarrow \mathbb{B} = [\{0,1\}; \vee, 0, \wedge, 1], \qquad n \longmapsto \begin{cases} 1 & \text{iff } n > 0 \\ 0 & \text{otherwise,} \end{cases}$$

$$\omega_{\oplus} : \mathbb{N} \longrightarrow \mathbb{F}_2 = [\{0,1\}; \oplus, 0, \wedge, 1], \qquad n \longmapsto \begin{cases} 1 & \text{iff } n \text{ is odd} \\ 0 & \text{otherwise,} \end{cases}$$

and, for each prime $p \in \mathbb{N}$,

$$\omega_p : \mathbb{N} \longrightarrow \mathbb{F}_p = [\{0, \ldots, p-1\}; +_{(mod\ p)}, 0, \cdot_{(mod\ p)}, 1], \qquad n \longmapsto n \ (\mathrm{mod}\ p).$$

Obviously,

- disjunctive $\{\vee\}$-branching programs are $\omega_\vee$-branching programs (they accept if at least one computation path is accepting),
- parity $\{\oplus\}$-branching programs are $\omega_\oplus$-branching programs (they accept if the number of accepting computation paths is odd), and
- MOD_p-branching programs, p prime, are ω_p-branching programs (they accept if the number of accepting computation paths equals 1 modulo p).

Due to this correspondence we immediately obtain the following characterization of the well-known nonuniform logarithmic space-bounded complexity classes $\mathcal{L} = L/poly$, $\mathcal{NL} = NL/poly$, $\oplus\mathcal{L} = \oplus L/poly$, $MOD_p\mathcal{L} = (MOD_pL)/poly$ by means of (sequences of) polynomial size ω-branching programs. Remember that the *size* of an ω-branching program P, $size(P)$, is the number of non-sink nodes of P. By $\mathcal{P}_{\omega-BP}$ we denote the complexity class of all languages A, $A \subseteq \mathcal{R}^*$, which are accepted by sequences of polynomial size ω-branching programs.

Proposition 1.
(1) $\mathcal{P}_{BP} = \mathcal{L}$ [PŽ83],
(2) $\mathcal{P}_{\omega_\vee-BP} = \mathcal{NL}$ [Mei88],
(3) $\mathcal{P}_{\omega_\oplus-BP} = \mathcal{P}_{\omega_2-BP} = \oplus\mathcal{L}$ [Mei88], and
(4) $\mathcal{P}_{\omega_p-BP} = MOD_p$-$\mathcal{L}$, p prime, [DKMW94]. $\square$

2 Bounded Alternating ω-Branching Programs

Let X be a set of variables over a finite semiring $\mathcal{R}$, and let $Y, Z \subseteq X$, $\#Y = \#Z = \varepsilon n$, $\varepsilon > 0$, be two disjoint subsets of X. An ω-branching program P, $\omega : I\!N \longrightarrow \mathcal{R}$ semiring homomorphism onto $\mathcal{R}$, that tests variables of X is said to be of *alternation length α with respect to Y and Z* if each path of P can be divided into α segments in which, alternating, variables of Y or variables of Z are *not* tested , and if α is minimal with this property. A sequence of ω-branching programs P_n is called *bounded alternating* if there exist two disjoint subsets $Y, Z \subseteq X$, $\#Y = \#Z = \varepsilon n$, $\varepsilon > 0$, such that P_n is of alternation length $n^{o(1)}$ with respect to Y and Z.

By $\mathcal{P}_{ba\ \omega-BP}$ we denote the set of languages $A, A \subseteq \mathcal{R}^*$ which are accepted by sequences of polynomial size, bounded alternating ω-branching programs. Observe that, since $\{0,1\} \subseteq \mathcal{R}$ for all semirings $\mathcal{R}$, $\{0,1\}$-languages can be considered in any case. For the particular semiring homomorphisms $\omega = \omega_\vee$, $\omega_\oplus$, ω_p(p prime), we write, due to Proposition 1, $\mathcal{NL}_{ba}$, $\oplus\mathcal{L}_{ba}$, and $MOD_p\mathcal{L}_{ba}$ instead of $\mathcal{P}_{ba\ \omega_\vee-BP}$, $\mathcal{P}_{ba\ \omega_\oplus-BP}$, and $\mathcal{P}_{ba\ \omega_p-BP}$, respectively.

Polynomial size, bounded alternating ω-branching programs seem to be quite powerful computation devices. For instance, the vast majority of arithmetic functions that can be computed by polynomial size branching programs can be computed by bounded alternating ones (in most cases with merely constant alternations). Even problems that are complete in the unrestricted logarithmic space–bounded complexity classes $\mathcal{L}$, $\mathcal{NL}$, $\oplus\ \mathcal{L}$, $MOD_p\mathcal{L}$ belong to the corresponding restricted bounded alternating classes.

Proposition 2 [MW91].

Let ω-GAP_{mon} denote the GRAPH ACCESSIBILITY PROBLEM that decides for a given acyclic monotone graph $G = (\{1,\ldots,n\},E)$ whether $\omega(\#[1 \xrightarrow{G} n]) = 1_\mathcal{R}$, where $\#[i \xrightarrow{G} j]$ denotes the number of paths from i to j in G. Then

1. ω-GAP_{mon} is p-projection complete in $\mathcal{P}_{\omega-BP}$, and

2. ω-$GAP_{\mathrm{mon}} \in \mathcal{P}_{ba\ \omega-BP}$. $\square$

Particularly, the monotone GRAPH ACCESSIBILITY PROBLEMs $GAP_{\mathrm{mon}}1$, $GAP_{\mathrm{mon}}2$, ODD-$PATH$-$GAP_{\mathrm{mon}}2$, and MOD_p-$GAP_{\mathrm{mon}}2$ (p prime) which, due to results of [Mei86, Mei89, DKMW94], are known to be p-projection complete in $\mathcal{L}$, $\mathcal{NL}$, $\oplus\mathcal{L}$, and $MOD_p\mathcal{L}$, respectively, belong to the corresponding bounded alternating classes $\mathcal{L}_{ba}$, $\mathcal{NL}_{ba}$, $\oplus\mathcal{L}_{ba}$, and MOD_p-$\mathcal{L}_{ba}$.

How do bounded alternating ω-branching programs fit into the environment of restricted types of branching programs investigated in the past? Beside of read-k times branching programs [BRS93] the most general type of branching programs for which up to now it was possible to establish exponential lower bounds without restricting its length by the number of input variables are oblivious programs of linear length [KMW89]. Remember that, an ω-branching program is said to be *oblivious* if it is leveled (i. e., all paths from the source of the program to any one of its nodes are of the same length) and the property that one node of a level is labeled with a variable x implies that all nodes of that level are labelled by x. A level whose nodes are labeled in this way is called an *input level.* The *length* of an oblivious branching program is the number of its input levels. The classes of all languages which are accepted by sequences of oblivious, polynomial size and linear length ω-branching programs are denoted by $\mathcal{P}_{\text{lin } \omega-BP_o}$.

Proposition 3.
Let ω be any of the semiring homomorphisms $\omega_\vee$, $\omega_\oplus$, or ω_p (p prime). Polynomial size bounded alternating ω-branching programs are strictly more powerful than polynomial size oblivious ω-branching programs of linear length. I. e.,

$$\mathcal{P}_{\text{lin } \omega-BP_o} \overset{\subset}{\neq} \mathcal{P}_{ba\ \omega-BP} \subseteq \mathcal{P}_{\omega-BP}.$$

Proof. (Omitted) $\square$

Finally let us consider the question whether the classes $\mathcal{P}_{ba\ \omega-BP}$ are closed under complement. Let

$$co\text{-}\mathcal{P}_{ba\ \omega-BP} = \{A \subseteq \mathcal{R}^* \mid (\mathcal{R}^* - A) \in \mathcal{P}_{ba\ \omega-BP}\}$$

be the co-class of the complexity class $\mathcal{P}_{ba\ \omega-PB}$. While we will see later that the class $\mathcal{NL}_{ba} = \mathcal{P}_{ba\ \omega-BP}$ is not closed with respect to complement the classes $MOD_p\mathcal{L}_{ba} = \mathcal{P}_{ba\ \omega_p-BP}$, p prime, are.

Proposition 4.
Let p be prime. Then

$$\mathcal{P}_{ba\ \omega_p-BP} = co\text{-}\mathcal{P}_{ba\ \omega_p-BP}.$$

Proof. Let P be a polynomial size ω_p-branching program. Adding $p-1$ accepting paths "for free" to P we obtain an ω_p-branching program P' with $acc_{P'}(a) \equiv 0 \pmod p$ iff P accepts a (and, consequently, $acc_{P'}(a) \not\equiv 0 \pmod p$ if a is not accepted by P). Now, taking $p-1$ copies $P_1, \ldots, P_{p-1}$ of P' and identifying, for all $i = 2, \ldots, p-1$, the 1-sink of P_{i-1} with the source of P_i we get a polynomial size ω_p-branching program P''. Since $acc_{P''}(a) = acc_{P'}(a)^{p-1}$ for each input a, $a \in I\!F_p^n$, a straight-forward application of FERMAT's Theorem shows that P'' computes 1 (0) on input a iff $acc_{P'}(a) \not\equiv 0 \pmod p$ $(acc_{P'}(a) \equiv 0 \pmod p)$ and, hence, iff P does not accept a (if P accepts a).

Obviously, P'' is bounded alternating if P is. $\square$

3 The Lower Bound Technique

Now we develop a lower bound technique that allows us to prove exponential lower bounds on the size of bounded alternating ω-branching programs. The lower bound proofs proceed in two steps. In the first step exponential lower bounds on the size of some specially structured bounded alternating ω-branching programs are derived. This is done by estimating certain ranks of communication matrices of a problem. Then, in a second step, it is proved that each polynomial size ω-branching program can be transformed into such a special ω-branching program of polynomial size preserving the 'bounded alternating'–property.

Let $\mathcal{R}$ be a finite semiring, and let $\omega : I\!N \longrightarrow \mathcal{R}$ be the semiring homomorphism onto $\mathcal{R}$. Let P be an ω-branching program with input variables from a set X, and let Y, Z be a partition of X, $Z = X - Y$. Let us consider the set V_X of nodes of P which are labeled with variables from $X = Y \cup Z$. A node v, $v' \in V_X$ is called a *predecessor* in V_X of a node v of P if there is a path in P from v' to v that does not contain any node of V_X. A node v of P is called a Y-Z-*alternation node* if it is labeled with a variable from Z and if all predecessors in V_X of v are labeled with variables from Y. An *alternation node* is a node that is either Y-Z-alternating or Z-Y-alternating. On the other hand, v is said to be *homogeneous* if all its predecessors in V_X are labeled either with variables from Y or Z and if v is not an alternation node. Introducing certain dummy nodes, at the cost of multiplying the size by the constant $\#\mathcal{R}$, P can be converted – without changing the alternation length – to an ω-branching program which consists merely of homogeneous or alternation nodes and accepts the same set. Hence, we assume all our ω-branching programs to consist merely of homogeneous and alternation nodes.

The *alternation depth* of a node v is the maximal number of alternation nodes on a path from the source to v. The alternation depth of the 1-sink v_1 is the *alternation length* of P.

An ω-branching program P is said to be (Y, Z)-*synchronous* if the alternation depth of two consecutive nodes of P differs at most by 1. Let P be a (Y, Z)-synchronous ω-branching program. All nodes of P with the same alternation depth form an (alternation) *segment.* The subsets of all alternation nodes with the same alternation depth are called *alternation levels.* Obviously, each alternation level consists either of Y-Z or of Z-Y-alternation nodes.

Our lower bound technique is mainly based on considerations of invariants of the *communication matrix* $M_{Y,Z}(f)$ of a function f. If $f : \mathcal{R}^Y \times \mathcal{R}^Z \longrightarrow \{0, 1\}$ then $M_{Y,Z}(f)$ is a $(\#\mathcal{R})^{\#Y} \times (\#\mathcal{R})^{\#Z}$ matrix which is defined, for $a_Y \in \mathcal{R}^Y$, $a_Z \in \mathcal{R}^Z$, by

$$(M_{Y,Z}(f))_{a_Y,a_Z} = f(a_Y, a_Z).$$

The matrix-invariants we work with are certain matrix-ranks. Remember that, if

$M \in I\!M_{\mathcal{R}}(n,m)$ is a $n \times m$ matrix over $\mathcal{R}$, then the *rank* of M over $\mathcal{R}$, $\mathrm{rank}_{\mathcal{R}}(M)$, is the minimum k such that M can be written as $M = A \cdot B$ with $A \in I\!M_{\mathcal{R}}(n,k)$ and $B \in I\!M_{\mathcal{R}}(k,m)$.

For simplicity we denote the addition in $\mathcal{R}$ by $+$, the multiplication by $\cdot$, and the standard inner product by $\langle .,. \rangle_{\mathcal{R}}$ or, even shorter, by $\langle .,. \rangle$.

Lemma 5.
Let Y, Z be a partition of X, and let P be a (Y,Z)-synchronous ω-branching program of alternation length α that computes a function $f : \mathcal{R}^X \longrightarrow \{0,1\}$. Then

$$\mathrm{Size}(P) \geq \Big(\mathrm{rank}_{\mathcal{R}} M_{Y,Z}(f)\Big)^{1/\alpha}.$$

Proof. Let $a \in R^X = R^Y \times R^Z$. By $\#[v \xrightarrow{a} v']$ we denote the number of paths leading in P under the input a from node v to node v'. Observe, that $\#[v_s \xrightarrow{a} v_1] = acc_P(a)$ and, hence, $f(a) = 1$ iff $\omega(\#[v_s \xrightarrow{a} v_1]) = 1_R$.

Suppose that the nodes at any alternation level r of P are numbered $v_{r,1}, v_{r,2}, \ldots, v_{r,\sigma(r)}$. Introducing dummy nodes we can assume that there is a σ, $\sigma \leq size(P)$, with $\sigma(r) = \sigma$ for all $r, 1 \leq r \leq \alpha$. An easy inductive argument yields, that, for all numbers $r \in \{1, \ldots, \alpha\}$ the set $\{v_{r,1}, \ldots, v_{r,\sigma}\}$ is a cut-set in P. That means

– there is no path from $v_{r,i}$ to $v_{r,j}$ if $i \neq j$,

– if P is any path from v_s to v_1 then the support of p contains one node $v_{r,i}$ for some i, $1 \leq i \leq \sigma$.

Now, for each alternation level r of P we define a *top vector* $t_r(a) \in I\!N^\sigma$ and a *bottom vector* $b_r(a) \in I\!N^\sigma$ by

$$t_r(a) = (\#[v_s \xrightarrow{a} v_{r,1}], \ldots, \#[v_s \xrightarrow{a} v_{r,\sigma}]),$$

$$b_r(a) = (\#[v_{r,1} \xrightarrow{a} v_1], \ldots, \#[v_{r,\sigma} \xrightarrow{a} v_1]),$$

For segments S_r of P, $1 \leq r < \alpha$, we define *segment matrices* $S_r(a) \in I\!M_{I\!N}(\sigma,\sigma)$ by

$$(S_r(a))_{i,j} = \#[v_{r,i} \xrightarrow{a} v_{r+1,j}].$$

Since, $\{v_{r,1}, \ldots, v_{r,\sigma}\}$ is a cut-set,

$$\#[v_s \xrightarrow{a} v_1] = \langle t_r(a), b_r(a) \rangle_{I\!N}$$

for each r, $1 \leq r < \alpha$, and, hence,

$$f(a) = 1 \text{ iff } \omega(\langle t_r(a), b_r(a) \rangle_{I\!N}) = 1_R.$$

Moreover, it follows from the cut-set property of $\{v_{r,1},\ldots,v_{r,\sigma}\}$ and $\{v_{r+1,1},\ldots,v_{r+1,\sigma}\}$ that

$$b_r(a) = S_r(a)\cdot b_{r+1}(a)$$

for each r, $1\le r<\alpha$. Hence, $\#[v_s \xrightarrow{a} v_1]$ can be computed by

$$\#[v_s \xrightarrow{a} v_1] = \langle t_1(a), S_1(a)\cdot S_2(a)\cdot\ldots\cdot S_{\alpha-1}(a)\cdot b_\alpha(a)\rangle_{\mathbb{N}}. \qquad (*)$$

W.l.o.g. let α be odd, and let segments S_{2i} (S_{2i-1}), $0<i\le(\alpha-1)/2$ depend merely on variables from Y (Z). If $a=a_Y a_Z$, $a_Y\in R^Y$, $a_Z\in R^Z$, then $(*)$ can be read as

$$\#[v_s \xrightarrow{a} v_1] = \langle t_1(a_Y), S_1(a_Z)\cdot S_2(a_Y)\cdot\ldots\cdot S_{\alpha-1}(a_Y)\cdot b_\alpha(a_Z)\rangle_{\mathbb{N}}.$$

Now let $M_{\alpha,\sigma}$ be the following $\#R^{(\sigma+\sigma^2(\alpha-1)/2)}\times\#R^{(\sigma+\sigma^2(\alpha-1)/2)}$ matrix:

$$(M_{\alpha,\sigma})_{(t,T_2,T_4,\ldots,T_{\alpha-1}),(b,B_1,B_3,\ldots,B_{\alpha-2})} = \langle t, B_1\cdot T_2\cdot\ldots\cdot T_{\alpha-1}\cdot b\rangle_R, \qquad (**)$$

$(t,T_2,\ldots,T_{\alpha-1}),(b,B_1,\ldots,B_{\alpha-2})\in R^\sigma\times[\mathbb{M}_R(\sigma,\sigma)]^{(\alpha-1)/2}$. Let $\{e_i \mid i=1,\ldots,\sigma\}$ and $\{E_{i,j}\mid i,j=1,\ldots,\sigma\}$ be the standard R–basis of R^σ and of $\mathbb{M}_R(\sigma,\sigma)$, respectively. Moreover, let us define the following set $\mathcal{I}=\{(e_i,E_{j_1,k_1},E_{j_3,k_3},\ldots,E_{j_{\alpha-2},k_{\alpha-2}})\mid i,j_1,k_1,\ldots j_{\alpha-2},k_{\alpha-2}=1,\ldots,\sigma\}$. Since the defining expression $(**)$ of the matrix $M_{\alpha,\sigma}$ is R–linear in each variable, an easy calculation yields that any column of the matrix $M_{\alpha,\sigma}$ is an R–linear combination of the columns indexed by elements of $\mathcal{I}$. It follows from the equation $\#\mathcal{I}=\sigma^\alpha$ that

$$\mathrm{rank}_R(M_{\alpha,\sigma})\le\sigma^\alpha.$$

If we take those rows and columns of $M_{\alpha,\sigma}$ for which there are assignments $a_Y\in R^Y$, $a_Z\in R^Z$ such that

$$t=\omega^\sigma(t_1(a_Y)),\qquad T_i=\omega^{\sigma^2}(S_i(a_Y))\qquad (i \text{ even }),$$

and

$$b=\omega^\sigma(b_\alpha(a_Z)),\qquad B_i=\omega^{\sigma^2}(S_i(a_Z))\qquad (i \text{ odd})$$

for the cartesian product $\omega^m:\mathbb{N}^m\longrightarrow R^m$, $m\in\mathbb{N}$, of the semiring homomorphism $\omega:\mathbb{N}\longrightarrow R$ then we obtain a submatrix M of $\omega^{\sigma+\sigma^2(\alpha-1)/2)}(M_{\alpha,\sigma})$ that possesses the same core as $M_{Y,Z}(f)$ does. Recall, the core of a matrix is the minimal submatrix such that every pair of rows and every pair of columns is different. Now

$$\mathrm{rank}_R(M)=\mathrm{rank}_R(M_{Y,Z}(f))$$

implies

$$\mathrm{rank}_R(M_{Y,Z}(f)) \leq \sigma^\alpha. \ \Box$$

Due to Lemma 5, lower bounds on the $\mathcal{R}$-rank of the communication matrix $M_{Y,Z}(f)$ provide lower bounds on the size of (Y,Z)-synchronous ω-branching programs. The following Lemma proves that such lower bounds also imply lower bounds on the size of arbitrary ω-branching programs.

Lemma 6.
Let (Y,Z) be a partition of X. Each ω-branching program P of size σ can be simulated by a (Y,Z)-synchronous ω-branching program P' of size σ^2.

Proof. Let $d(v)$ denote the alternation depth of node v of P, and, for $v \in V_X$, let $t(v)$ denote the variable which is tested in v. Further, let $a_Y \in R^Y$, and $a_Z \in R^Z$ be arbitrarily fixed.

Consider an edge (u,v) of P with $d(v)-d(u) > 1$. Let $\tilde{t}(v)$ by any one of the variables that are tested in a predecessor in V_X of v. Since P was assumed to consist merely of alternation or of homogeneous nodes all these variables and, hence, $\tilde{t}(v)$ belong either exclusively to Y or exclusively to Z. Now, starting with the source and replacing each edge (u,v) of P with $d(v)-d(u) > 1$ by the branching-program-construct

$$P_{d(u)-d(v),u,v}$$

given in Figure 2 we obtain an ω-branching program P' that is (Y,Z)-synchronous. Since, obviously, P' accepts the same set as P does, and since $Size(P') \leq Size(P)^2$ we are done. $\Box$

Of particular importance for the following is the fact that is suffices to apply the lower bound technique developed in Lemmas 5 and 6 merely to certain subfunctions of a function f in order to derive exponential lower bounds on the size of ω-branching programs for f. If Y, $Z \subseteq X$ are disjoint subsets of X, and if $c \in \mathcal{R}^{X-(Y\cup Z)}$, then we denote by $f^c : \mathcal{R}^{Y\cup Z} \longrightarrow \{0,1\}$ the subfunction $f^c(y,z) := f(c,y,z)$ for all $y \in \mathcal{R}^Y$, $z \in \mathcal{R}^Z$.

Theorem 7.
Let $f : \mathcal{R}^X \longrightarrow \{0,1\}$ be a function, Y, $Z \subseteq X$ two disjoint subsets of X, and P an ω-branching program of alternation length α with respect to Y and Z that computes f. Then

$$Size(P) \geq (rank_{\mathcal{R}} M_{Y,Z}(f^c))^{1/2\alpha}$$

for each $c \in \mathcal{R}^{X-(Y \cup Z)}$.

Proof. "Hardwiring" the variables of $X-(Y \cup Z)$ according to c from P we obtain an ω-branching program P' of alternation length α with respect to Y and Z that computes f^c over $X' = Y \cup Z$. Since Y, Z is a partition of X', due to Lemma 6, there is a (Y,Z)-synchronous ω-branching program P'' of alternation length α that computes f^c with

$$Size(P'') \le Size(P')^2 \le Size(P)^2.$$

Due to Lemma 5, we have

$$Size(P'') \ge (rank_R\ M_{Y,Z}(f^c))^{1/\alpha}\ . \ \Box$$

4 Lower Bounds on the Rank of Communication Matrices

Due to Theorem 7, in order to derive exponential lower bounds on the size of bounded alternating branching programs if suffices to derive exponential lower bounds on the rank of certain communication matrices.

Let us start with an easy observation concerning the SEQUENCE EQUALITY TEST SEQ= $\{\mathrm{SEQ}_{2n}\}$,

$$\mathrm{SEQ}_{2n} : \mathcal{R}^Y \times \mathcal{R}^Z \longrightarrow \{0,1\},$$

$\#Y = \#Z = n$, defined by

$$\mathrm{SEQ}_{2n}(y,z) = 1 \text{ iff } y = z.$$

Proposition 8.
Let $\mathcal{R}$ *be a finite semiring. Then it holds*

$$rank_{\mathcal{R}} M_{Y,Z}(\mathrm{SEQ}_{2n}) = \exp(\Omega(n)).$$

Proof. Obviously, $M_{Y,Z}(\mathrm{SEQ}_{2n})$ is the $\#R^n \times \#R^n$ identity matrix and, hence, of full rank over each semiring R. $\Box$

Now let $\omega : I\!N \longrightarrow \mathcal{R}$ be a semiring homomorphism and consider the ω-ORTHOGONALITY TEST ω-ORT $= \{\omega\text{-ORT}_{2n}\}$,

$$\omega\text{-ORT}_{2n} : \mathcal{R}^Y \times \mathcal{R}^Z \longrightarrow \{0,1\},$$

$\#Y = \#Z = n$, defined by

$$\omega\text{-ORT}_{2n}(y,z) = 1 \text{ iff } \langle y,z\rangle_{\mathcal{R}} = O_{\mathcal{R}}. \quad \square$$

Proposition 9.
Let p, q primes with $p \neq q$. Then it holds

$$rank_{I\!F_q} M_{Y,Z}(\omega_p\text{-ORT}_{2n}) = \exp(\Omega(n)).$$

Proof. Let us represent each 1-dimensional subspace of $I\!F_p^n$ by a nontrivial vector and consider the submatrix M of $M_{Y,Z}(\omega_p\text{-ORT}_{2n})$ that is defined by these vectors. Obviously, M is a $m \times m$ matrix with

$$m = (p^n - 1)/(p-1) = 1 + p + \ldots + p^{n-1} = 2^{\Omega(n)}.$$

We prove that, for infinitely many n, M^2 is invertible (over $I\!F_q$) and, hence, of rank

$$m = 2^{\Omega(n)}.$$

For the moment consider M to be an integer matrix. Since

$$(M^2)_{y,z} = \#\{x \mid \omega_p\text{-ORT}_{2n}(y,x) = 1 \text{ and } \omega_p\text{-ORT}_{2n}(x,z) = 1\}$$

we obtain

$$(M^2)_{y,y} = (p^{n-1} - 1)/(p-1) =: a$$

and

$$(M^2)_{y,z} = (p^{n-2} - 1)/(p-1) =: b, \qquad y \neq z.$$

Consequently, M is a matrix of the form

$$M^2 = \begin{pmatrix} a & & & \\ & \ddots & b & \\ & b & \ddots & \\ & & & a \end{pmatrix}.$$

It is well known that, if it exists, the inverse of such a matrix is of the same shape. Now, easy computations show that M^2 is invertible (over $\mathbb{F}_q$) iff

$$p^{n-2} + m \cdot b \not\equiv 0 \pmod q.$$

Anyway, for n with

$$n \equiv 0 \pmod q \text{ and } n \equiv 2 \pmod{q-1} \qquad (*)$$

it holds $m \cdot b \equiv 0 \pmod q$ and, hence, $p^{n-2} + m \cdot b \not\equiv 0 \pmod q$. Indeed, due to FERMAT's theorem we have $p^{n-2} \equiv p^{\lambda(q-1)} \equiv 1 \pmod q$, $\lambda \in \mathbb{N}$. Now, $p \equiv 1 \pmod q$ yields $m = 1 + p + \ldots + p^{n-1} \equiv n \equiv 0 \pmod q$, and $p \not\equiv 1 \pmod q$ implies $b = (p^{n-2} - 1)/(p-1) \equiv 0 \pmod q$.

Since $\gcd(q, q-1) = 1$ there are infinitely many $n \in \mathbb{N}$ satisfying (*). Hence,

$$\exp(\Omega(n)) = m = \operatorname{rank}_{\mathbb{F}_q}(M) \le \operatorname{rank}_{\mathbb{F}_q}(M_{Y,Z}(\omega_p\text{-ORT}_{2n})). \ \square$$

Proposition 10.
Let p be prime. Then it holds

$$\operatorname{rank}_{\mathbb{B}} M_{Y,Z}(\omega_p\text{-ORT}_{2n}) = \exp(\Omega(n)).$$

Proof. Again, we represent each 1-dimensional subspace of $\mathbb{F}_p^n$ by a nontrivial vector and consider the $m \times m$ submatrix M of $M_{Y,Z}(\omega_p\text{-ORT}_{2n})$, $m = (p^n - 1)/(p-1)$, that is defined by these vectors.

Let $M|_{A \times B}$ be a 1-homogeneous submatrix of M, i. e. a submatrix whose entries are equal to 1 . Since $\omega_p\text{-ORT}_{2n}(a, b) = 1$ for any $a \in A$, $b \in B$ we have $\omega_p\text{-ORT}_{2n}(a, x) = 1$ for all vectors x from the linear subspace $\mathcal{L}(B)$ generated by B. Consequently, the vectors $a \in A$ are elements of the orthogonal complement $\mathcal{L}(B)^\perp$ of $\mathcal{L}(B)$. Hence,

$$\#A \cdot \#B \le (p^{n-k} - 1) \cdot (p^k - 1)/(p-1)^2$$

with $k = \dim \mathcal{L}(B)$. Since

$$(p^{n-k} - 1) \cdot (p^k - 1)/(p-1)^2 \le [(p^{\lceil n/2 \rceil} - 1)/(p-1)]^2,$$

we can estimate, for even n, the size of each 1–homogeneous submatrix of M by

$$\#A \cdot \#B \le [(p^{n/2} - 1)/(p-1)]^2.$$

Now we are done. Since the number of 1–entries in M equals

$$(p^n - 1)(p^{n-1} - 1)/(p-1)^2$$

and since each 1–entry of M has to be covered by at least one 1–homogeneous submatrix of M we have

$$\begin{aligned} \mathrm{rank}_{\boldsymbol{B}}(M_{Y,Z}(\omega_p\text{-ORT}_{2n})) &\geq \mathrm{rank}_{\boldsymbol{B}}(M) \\ &\geq (p^n - 1)(p^{n-1} - 1)/(p^{n/2} - 1)^2 \\ &\geq \exp(\Omega(n)). \ \square \end{aligned}$$

5 Lower Bounds on the Size of Bounded Alternating ω-Branching Programs

The lower bounds on the $\mathcal{R}$-rank of the communication matrices derived in the last section imply, due to Theorem 7, exponential lower bounds on the size of bounded alternating ω-branching programs.

Let $F = \{f_n\}$ be a sequence of functions,

$$f_n : \mathcal{R}^n \longrightarrow \{0,1\},$$

and let æ be a symbol not contained in $\mathcal{R}$. Obviously, F is a subproblem of the problem $F^{æ} = \{f_n^{æ}\}$,

$$f_n^{æ} : (\mathcal{R} \cup \{æ\})^n \longrightarrow \{0,1\}$$

defined by

$$f_n^{æ}(a) = 1 \quad \text{iff } red(a) \text{ is of even length } 2m \text{ and } f_{2m}(red(a)) = 1,$$

where $red(a) \in \mathcal{R}^*$ denotes the *reduced word* of a obtained from a by deleting all occurences of æ in a.

Now we consider the æ-extension $\mathrm{SEQ}^{æ} = \{\mathrm{SEQ}_{2n}^{æ}\}$ of the SEQUENCE EQUALITY PROBLEM and the æ-extension $\omega_p\text{-ORT}^{æ} = \{\omega_p\text{-ORT}_{2n}^{æ}\}$, p prime, of the ω_p-ORTHOGLONALITY TEST.

Proposition 11.
Let $\mathcal{R}$ be a finite semiring, and let $\omega : I\!N \longrightarrow \mathcal{R}$ be a semiring homomorphism. If P is a bounded alternating ω-branching program that computes $\mathrm{SEQ}_{2n}^{æ}$ then

$$Size(P) = \exp(\Omega(n)).$$

Proof. Let $X = \{x_1, \ldots, x_{2n}\}$, and let P be a bounded alternating ω-branching program that computes $\mathrm{SEQ}_{2n}^{æ}$ over X. Hence there are two disjoint sets Y, $Z \subseteq X$, $\#Y = \#Z = \lfloor \varepsilon n \rfloor$, $\varepsilon > 0$, such that P is of alternating length $n^{o(1)}$ with respect to Y and Z. Since $c \in \{æ\}^{X-(Y \cup Z)}$ defines a subprogram P' of P that computes $\mathrm{SEQ}_{2\lfloor \varepsilon n \rfloor}$ for each $a_Y \in R^Y$, $a_Z \in R^Z$, we obtain

$$Size(P) = \exp(\Omega(\varepsilon n)) = \exp(\Omega(n))$$

due to Theorem 7 and Proposition 8. $\Box$

Similarly, due to Theorem 7 and Propositions 9 and 10 one obtains the following results.

Proposition 12.
Let p, q primes with $p \neq q$. If P is a bounded alternating ω_q-branching program that computes ω_p-$\mathrm{ORT}_{2n}^{æ}$ then

$$Size(P) = \exp(\Omega(n)). \ \Box$$

Proposition 13.
Let p be prime. If P is a disjunctive bounded alternating $\omega_\vee$-branching program that computes ω_p-$\mathrm{ORT}_{2n}^{æ}$ then

$$Size(P) = \exp(\Omega(n)). \ \Box$$

6 Separation Results

Now, combining the exponential lower bounds obtained in Section 5 with some polynomial upper bounds we are able to establish strong differences in the computational power of bounded alternating ω-branching programs for different ω. These differences imply, in particular, separation results on the corresponding logarithmic space-bounded complexity classes $\mathcal{L}_{ba}$, $\mathcal{NL}_{ba}$, *co*-$\mathcal{NL}_{ba}$, $\oplus\mathcal{L}_{ba}$, and MOD_p-$\mathcal{L}_{ba}$, p prime.

We start with giving a polynomial upper bound on the size of (sequences of) disjunctive $\omega_\vee$-branching programs that compute $\neg\mathrm{SEQ}^{æ}$.

Proposition 14.
$\neg\mathrm{SEQ}^{æ}_{2n}$ can be computed by means of a disjunctive $\omega_\vee$-branching program of size $O(n^4)$ and alternation length 3.

Proof. (Omitted) $\square$

Next we can give a polynomial upper bound on the size of (sequences of) ω_p-branching programs that compute ω_p-$\mathrm{ORT}^{æ}$.

Proposition 15.
Let p be prime. Then ω_p-$\mathrm{ORT}^{æ}_{2n}$ can be computed by means of a ω_p-branching program of size $O(n^4)$ and alternation length 3.

Proof. (Omitted) $\square$

Altogether, the lower bounds of Propositions 11 – 13 and the upper bounds of Propositions 14 – 15 imply the following corollary.

Corollary 16.
(1) $SEQ^{æ} \notin \mathcal{P}_{ba\ \omega-BP}$ for each ω. Hence, $SEQ^{æ} \notin \mathcal{P}_{ba\ BP}$.
(2) $\neg SEQ^{æ} \in \mathcal{P}_{ba\ \omega_\vee-BP}$.
(3) ω_p-$ORT^{æ} \notin \mathcal{P}_{ba\ \omega_\vee-BP}$, p prime. Hence, ω_p-$ORT^{æ} \notin \mathcal{P}_{ba\ BP}$.
(4) ω_p-$ORT^{æ} \notin \mathcal{P}_{ba\ \omega_q-BP}$, p, q primes, $p \neq q$.
(5) ω_p-$ORT^{æ} \in \mathcal{P}_{ba\ \omega_p-BP}$, p, prime. $\square$

Since the classes MOD_p-$\mathcal{L}_{ba}$, due to Proposition 4, are closed under complement, and since, due to Propositions 11 and 14, the class $\mathcal{NL}_{ba}$ is not, the bounds of Corollary 16 provide the following separation results concerning the complexity classes $\mathcal{L}_{ba}$, $\mathcal{NL}_{ba}$, *co*-$\mathcal{NL}_{ba}$, $\oplus\mathcal{L}_{ba}$, and MOD_p-$\mathcal{L}_{ba}$, $p > 2$ prime, defined by bounded alternating $\omega_\vee$-branching programs and ω_p-branching programs.

Theorem 16.
(1) Any two complexity classes $\mathcal{K}$ and $\mathcal{K}'$

$$\mathcal{K}, \mathcal{K}' \in \{\mathcal{NL}_{ba}, co\text{-}\mathcal{NL}_{ba}, \oplus\mathcal{L}_{ba}, MOD_p\mathcal{L}_{ba}(p > 2 \ prime)\}$$

are uncomparable via inclusion, i. e.

$$\mathcal{K} \not\subseteq \mathcal{K}' \text{ and } \mathcal{K}' \not\subseteq \mathcal{K}.$$

(2) Each of these classes properly contain the complexity class $\mathcal{L}_{ba}$.

(3) Finally, the classes $\mathcal{NL}_{ba}$ and co-$\mathcal{NL}_{ba}$ are properly contained in $\mathcal{NL}$,

$$\mathcal{NL}_{ba}, co\text{-}\mathcal{NL}_{ba} \subsetneq \mathcal{NL},$$

i. e. unbounded alternating disjunctive branching programs are strictly more powerful than bounded alternating ones. □

References

[AM86] N. Alon, W. Maass: Meanders, Ramsey theory and lower bounds, Proc. 27th ACM STOC, 1986, 30–39.

[BRS93] A. Borodin, A. Razborov, R. Smolensky: On lower bounds for read-k times branching programs, Comput. Complexity 3 (1993), 1-18.

[DKMW94] D. Damm, M. Krause, Ch. Meinel, S. Waack: Separating Oblivious Linear Length MOD_p–Branching Program Classes, J. Inform. Process. Cybernet. EIK 30 (1994) 2, 63–75.

[KMW89] M. Krause, Ch. Meinel, S. Waack: Separating Complexity Classes Related to Certain Input Oblivious Logarithmic Space Bounded Turing Machines, Proc. 4th IEEE Structure in Complexity Theory, 1989, 240–259.

[Kra90] M. Krause: Separating $\oplus\mathcal{L}$ from $\mathcal{L}$, $co\text{-}\mathcal{NL}$ and $AL = P$ for Oblivious Turing Machines of Linear Access Time, Proc. MFCS'90, LNCS 452, 385–391.

[Lee59] C. Y. Lee: Representation of Switching Functions by Binary Decision Programs, Bell System Techn. Journal 38 (1959), 985–999.

[Mei88] Ch. Meinel: Polynomial Size Ω-Branching Programs and Their Computational Power, Proc. STACS'88, LNCS 294, 81–90.

[Mei89] Ch. Meinel: Modified Branching Programs and Their Computational Power, LNCS 370, Springer Verlag, 1989.

[MW91] Ch. Meinel, S. Waack: Upper and Lower Bounds for Certain Graph-Accessibility-Problems on Bounded Alternating Branching Programs, MFCS'91, LNCS 520, 337–345.

[MW93] CH. Meinel, S. Waack: Separating Complexity Classes Related to Bounded Alternating ω-Branching Programs, ISAAC'93, LNCS 762, 379–388. To appear in Math. Systems Theory 27.

[PŽ83] P. Pudlák, S. Žak: Space Complexity of Computations, Preprint Univ. of Prague, 1983.

[Žak84] S. Žak: An Exponential Lower Bound for One-Time-Only Branching Programs, Proc. MFCS'84, LNCS 176, 562–566.