

Improved bounds for reduction to depth 4 and depth 3



Sébastien Tavenas

LIP, École Normale Supérieure de Lyon, UMR 5668 ENS Lyon – CNRS – UCBL – INRIA, Université de Lyon, France

ARTICLE INFO

Article history:

Received 26 September 2013

Available online 2 October 2014

Keywords:

Arithmetic circuit

Parallelization

ABSTRACT

Koiran showed that if an n -variate polynomial f_n of degree d (with $d = n^{O(1)}$) is computed by a circuit of size s , then it is also computed by a homogeneous circuit of depth four and of size $2^{O(\sqrt{d} \log(n) \log(s))}$. Using this result, Gupta, Kamath, Kayal and Saptharishi found an upper bound for the size of a depth three circuit computing f_n .

We improve here Koiran's bound. Indeed, we transform an arithmetic circuit into a depth four circuit of size $2^{O(\sqrt{d} \log(ds) \log(n))}$. Then, mimicking the proof in [2], it also implies a $2^{O(\sqrt{d} \log(ds) \log(n))}$ upper bound for depth three circuits.

This new bound is almost optimal since a $2^{\Omega(\sqrt{d})}$ lower bound is known for the size of homogeneous depth four circuits such that gates at the bottom have fan-in at most \sqrt{d} . Finally, we show that this last lower bound also holds if the fan-in is at least \sqrt{d} .

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

Valiant, Skyum, Berkowitz and Rackoff [4] proved that if a size- s depth- d circuit computes a polynomial of degree d , then this polynomial can also be computed by a circuit of depth $O(\log(d) \log(s))$ and of size bounded by a polynomial in s (this result will be the basis for the parallelization in this paper). Some years later, Allender, Jiao, Mahajan and Vinay [5] studied this parallelization method and showed it could be done uniformly. Using the proof of these results, Agrawal and Vinay proved [6] that if an n -variate polynomial f of degree $d = O(n)$ has a circuit of size $2^{o(d + d \log(\frac{n}{d}))}$, then f can also be computed by a depth-four circuit ($\sum \prod \sum \prod$) of size $2^{o(d + d \log(\frac{n}{d}))}$. This result shows that for proving arithmetic circuit lower bounds or black-box derandomization of identity testing, the case of depth four arithmetic circuit is the general case in a certain sense.

The hypothesis of Agrawal and Vinay's result is quite weak: they consider circuits of size $2^{o(d + d \log(\frac{n}{d}))}$ (we can notice that all polynomials have a formula of size $d \binom{n+d}{d} = 2^{O(d \log(\frac{n+d}{d}))}$). But if the hypothesis is strengthened, it is possible to get a stronger conclusion. Indeed, Koiran [1] showed that if a circuit is of size s , then it can be computed by a homogeneous depth-four circuit of size $2^{O(\sqrt{d} \log(d) \log(s))}$. For example, if the permanent family is computed by a polynomial size circuit (i.e., of size n^c), then it is computed by a depth-four circuit of size $2^{O(\sqrt{n} \log^2(n))}$. These results appear as an interesting approach to lower bounds: if one finds a $2^{\omega(\sqrt{n} \log^2(n))}$ lower bound on the size of $\sum \prod^{[O(\sqrt{n})]} \sum \prod^{[\sqrt{n}]}$ circuits computing the permanent, then it will imply that there are no polynomial size circuits for the permanent. Moreover it could be easier to find lower bounds on the size of these particular circuits than for the general circuits. Indeed, although no superpolynomial lower bound is known for general circuits, Gupta, Kamath, Kayal and Saptharishi [3] get a nearly optimal lower bound for particular depth-4 circuits for the permanent. More precisely, they showed that if a homogeneous $\sum \prod \sum \prod$

E-mail address: sebastien.tavenas@ens-lyon.org.

circuit where the bottom fan-in is bounded by t computes the permanent of a matrix of size $n \times n$, then its size is $2^{\Omega(\frac{n}{t})}$. In particular, a $\sum \prod^{[O(\sqrt{n})]} \sum \prod^{[\sqrt{n}]}$ circuit computing the permanent is of size $2^{\Omega(\sqrt{n})}$. The following year, the same authors [2] improve the upper bound by transforming n -variate circuits of size s and depth d ($= n^{O(1)}$) into depth-3 circuits of size $2^{O(\sqrt{d \log s \log n \log d})}$, moreover if the input is a branching program (and not a circuit), the upper bound becomes $2^{O(\sqrt{d \log s \log n})}$. In particular, this result gives a depth-3 circuit of size $2^{O(\sqrt{n \log n})}$ computing the determinant of a matrix $n \times n$. Nevertheless, this result is not comparable to the depth-4 reductions since the depth-3 circuit they get is not homogeneous, and uses gates computing polynomials of very high degree. Very recently, Fournier, Limaye, Malod and Srinivasan [7] showed a $2^{\Omega(\sqrt{d/t \log n})}$ -lower bound for the size of the $\sum \prod \sum \prod$ circuits, with bottom fan-in bounded by t , which compute the iterated matrix multiplication.

In this paper we improve Koiran's bound. We show that a circuit of size s can be parallelized homogeneously in depth 4 and in size $2^{O(\sqrt{d \log(ds) \log(n)})}$ such that the fan-in of each multiplication gate is bounded by $O(\sqrt{d \frac{\log ds}{\log n}})$. We can notice that as $n \leq s$, the result implies Koiran's bound and is generally better (in the case where $d, s = n^{O(1)}$, Koiran's bound is $2^{O(\sqrt{n \log^2 n})}$ while the new bound is $2^{O(\sqrt{n \log n})}$). It implies that a $2^{\omega(\sqrt{n \log(n)})}$ lower bound for depth-4 circuits computing the permanent gives a super-polynomial lower bound for general circuits computing the permanent. Moreover, using this result in Gupta, Kamath, Kayal and Saptharishi's proof instead of Koiran's result slightly improves the depth-3 upper bound. An n -variate circuit of size s and depth d is computed by a depth-3 circuit of size $2^{O(\sqrt{d \log(ds) \log n})}$. So, we get the same bound for the reduction at depth 3 starting from an arithmetic circuit as from an arithmetic branching program. Finally in Section 7, we show, by a counting argument, that if a homogeneous $\sum \prod \sum \prod$ circuit where the bottom fan-in is lower-bounded by t computes the permanent (or the determinant) of a matrix of size $n \times n$, then its size is $2^{\Omega(t \log n)}$.

2. Arithmetic circuits

We give here a brief introduction to the theory of arithmetic circuits. The reader can find more detailed information in [8–11]. In this theory, we measure the complexity of polynomial functions using arithmetic circuits.

Definition 1. An arithmetic circuit is a finite acyclic directed graph with vertices of in-degree 0 or more and exactly one vertex of out-degree 0. Vertices of in-degree 0 are called inputs and labeled by a constant or a variable. The other vertices are labeled by \times or $+$ (or sometimes by \odot in this paper) and called computation gates (the in-degree of these gates will be also called the fan-in). The vertex of out-degree 0 is called the output. The vertices of a circuit are commonly called gates and its edges arrows. Finally, we call a formula, an arithmetic circuit such that the underlying graph is a tree.

A \odot -gate corresponds to a multiplication-by-a-scalar gate. The fan-in of such a gate will be always 2 and at least one of its inputs corresponds to a constant (we will give a syntactic restriction just after the next definition).

Each gate of a circuit computes a polynomial (defined by induction). The polynomial computed by a circuit corresponds to the polynomial computed by the output of this circuit. For a gate α , we denote $[\alpha]$ the polynomial computed by this gate. In fact, for some proofs, we will use circuits with several outputs (each one corresponds to an out-degree 0 gate).

Definition 2. The size of a circuit is its number of gates. The depth is the maximal length of a directed path from an input to an output. The degree of a gate is defined recursively: constant inputs labelled by 0 are of degree $-\infty$, other constant inputs are of degree 0, any variable input is of degree 1, the degree of a $+$ -gate is the maximum of the incoming degrees and the degree of a \times -gate (or a \odot -gate) is the sum of the incoming degrees.

A circuit is called *homogeneous* if for each $+$ -gate α , all the inputs of α have same degree.

We can now put a restriction for the \odot -gates. For each one of these gates, one of its two children has to be of degree 0.

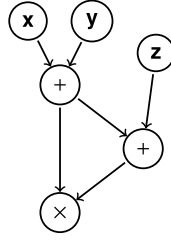
Remark 3. In the following, we will assume that the computation gates will never compute the zero polynomial. If it is the case, it is sufficient to replace this gate by an input gate labelled by the constant 0.

For a given circuit we will consider graphs called parse trees. A parse tree corresponds, in the spirit, to the computation of one particular monomial.

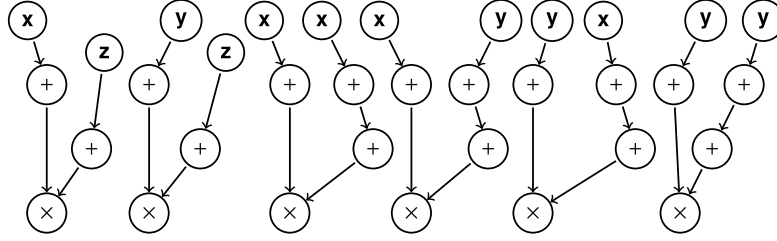
Definition 4. The set of parse trees of a circuit C is defined by induction on its size:

- If C is of size 1 it has only one parse tree, itself.
- If the output gate o of C is a $+$ -gate whose inputs are the gates $\alpha_1, \dots, \alpha_k$, then the parse trees of C are obtained by choosing, for an arbitrary $i \leq k$, a parse tree of the sub-circuit rooted in α_i and the arrow from α_i to the output o .
- If the output gate o of C is a \times -gate or a \odot -gate whose inputs are the gates $\alpha_1, \dots, \alpha_k$, the parse trees of C are obtained by taking for each $i \leq k$, one disjoint copie of a parse tree of the sub-circuit rooted in α_i , and the arrows from all α_i to the output o .

For example, the following circuit



has six parse trees.



We can notice that the size of a parse tree can be exponentially larger than the one of the original circuit. It will not be a problem in this paper. However, it is possible to avoid this increase using multiplicatively disjoint circuits as it is done in [12].

At each parse tree, we can associate the monomial which corresponds to the product of the leaves.

The next lemma is proved in [12].

Lemma 5. A polynomial f computed by a circuit C equals the sum of the monomials of the parse trees:

$$f = \sum_{T \text{ parse tree}} m(T)$$

where $m(T)$ is the monomial associated to the tree T .

We will use some convenient notations which are defined in [2]. A depth-4 circuit such that gates are multiplication gates at level one and three and addition gates at levels two and four are denoted $\Sigma\P\Sigma\P$ circuits. Furthermore, a $\Sigma\P^{[\alpha]}\Sigma\P^{[\beta]}$ circuit is a $\Sigma\P\Sigma\P$ circuit such that the fan-in of the multiplication gates at level 3 is bounded by α , and the fan-in of the multiplication gates at level 1 is bounded by β . For example, a $\Sigma\P^{[\alpha]}\Sigma\P^{[\beta]}$ circuit computes a polynomial of the form:

$$\sum_{i=1}^t a_i \prod_{j=1}^{u_{i,j}} \prod_{k=1}^{b_{i,j,k}} x_{i,j,k,l}$$

where $a_i \leq \alpha$, $b_{i,j,k} \leq \beta$.

Finally, in the following, we want to transform some circuits. The underlying ring will be the same for the new circuit. Moreover, it can be noticed that the following results (except for Proposition 8 and Corollary 9) hold for any commutative ring.

3. Upper bounds

Here, we state the main theorem of this paper.

Theorem 6. Let f be an n -variate polynomial computed by a circuit of size s and of degree d . Then f is computed by a $\Sigma\P^{[O(\alpha)]}\Sigma\P^{[\beta]}$ circuit C of size $2^{O(\sqrt{d \log(ds) \log n})}$ where $\alpha = \sqrt{d \frac{\log n}{\log ds}}$ and $\beta = \sqrt{d \frac{\log ds}{\log n}}$. Furthermore, if f is homogeneous, it will be also the case for C .

The previous theorem can be directly applied for the permanent.

Theorem 7. *If the $n \times n$ permanent is computed by a circuit of size polynomial in n , then it is also computed by a $\sum \prod^{[O(\sqrt{n})]} \sum \prod^{[O(\sqrt{n})]}$ circuit of size $2^{O(\sqrt{n} \log(n))}$.*

In their paper [2], Gupta, Kamath, Kayal and Saptharishi used the previous $2^{\sqrt{d} \log^2(s)}$ bound [1] for parallelizing at depth 3. They showed that:

Proposition 8. *(See Theorem 1.1 in [2].) Let $f(x) \in \mathbb{Q}[x_1, \dots, x_n]$ be an n -variate polynomial of degree $d = n^{O(1)}$ computed by an arithmetic circuit of size s . Then it can also be computed by a $\sum \prod \sum$ circuit of size $2^{O(\sqrt{d} \log n \log s \log d)}$ with coefficients coming from \mathbb{Q} .*

In fact, their proof is divided into three parts. First they transform circuits into depth-4 circuits, then they transform depth-4 circuits into depth-5 circuits using only sum and exponentiation gates. And finally they transform these last circuits into depth-3 circuits. Using Theorem 6 instead of Theorem 4.1 in their paper improves the first part of their proof. That implies a small improvement of Theorem 1.1 in [2]:

Corollary 9. *Let $f(x) \in \mathbb{Q}[x_1, \dots, x_n]$ be an n -variate polynomial of degree $d = n^{O(1)}$ computed by an arithmetic circuit of size s . Then it can also be computed by a $\sum \prod \sum$ circuit of size $2^{O(\sqrt{d} \log n \log s)}$ with coefficients coming from \mathbb{Q} .*

Finally, the use of the rationals is important in the third part of their proof. It will not be important in this paper.

4. Useful propositions

For proving Theorem 6, we will need the following propositions.
The next result is folklore. A proof can be found in [5].

Proposition 10. *If f is a degree- d polynomial computed by a $\{+, \times\}$ -circuit C of size s such that the fan-in of each $+$ -gate is unbounded and the fan-in of each \times -gate is bounded by 2, then there exists a circuit \tilde{C} of size $s(d+1)^2$ with $d+1$ outputs O_0, O_1, \dots, O_d such that:*

- the fan-in of each $+$ -gate is unbounded,
- the fan-in of each \times -gate is bounded by 2,
- for each i , the gate O_i computes the homogeneous part of f of degree i ,
- \tilde{C} is homogeneous,

Lemma 11. *In a homogeneous circuit, all the gates compute homogeneous polynomials. Moreover, the degree of each gate equals the degree of the homogeneous polynomial computed by this gate.*

Proof. We show this lemma by induction on the underlying graph.

- The lemma is true for all the input gates.
- If α is a $+$ -gate of inputs $\alpha_1, \dots, \alpha_p$, then by homogeneity, these inputs have the same degree d . By induction hypothesis, the gates $\alpha_1, \dots, \alpha_p$ compute some homogeneous polynomials of degree d . So $[\alpha]$ is a homogeneous polynomial of degree d or $-\infty$. By the Remark 3, the degree of $[\alpha]$ is d .
- If α is a \times -gate (or a \odot -gate) of inputs $\alpha_1, \dots, \alpha_p$, then by induction hypothesis the polynomials $[\alpha_1], \dots, [\alpha_p]$ are homogeneous and their degrees correspond to the degrees of $\alpha_1, \dots, \alpha_p$. Hence $[\alpha]$ is homogeneous and the degree of $[\alpha]$ equals the degree of α . \square

We define \times -balanced $\{\times, +, \odot\}$ -circuits.

Definition 12. A $\{\times, +, \odot\}$ -circuit C is called \times -balanced if and only if all the following properties are verified:

- the fan-in of each \times -gate is at most 5,
- the fan-in of each $+$ -gate is unbounded,
- the fan-in of each \odot -gate is at most 2,
- for each \times -gate α , each one of its arguments is of degree at most half of the degree of α .

The last condition cannot be true for the multiplication by a scalar. It is the reason, we introduced the operator \odot .

The next proposition was found by Agrawal and Vinay [6]. It slightly strengthens Valiant, Skyum, Berkowitz and Rackoff's famous result [4] by adding a constraint on all the \times -gates.

Proposition 13. Let f be a homogeneous degree- d polynomial computed by a size- s circuit \tilde{C} verifying the four points of the conclusion of Proposition 10. Then f is computed by a homogeneous \times -balanced $\{\times, +, \odot\}$ -circuit of size $s^6 + s^4 + 1$ and of degree d .

We present a proof of it in Section 5 as the statement above is slightly different from the one we can find in [6] or in [10] (the constants are a bit improved).

Corollary 14. Let f be a polynomial of degree d computed by a circuit of size s . Then f is computed by a $\{+, \times\}$ -circuit of size $(sd)^{O(1)}$ and of depth $O(\log(s) \log(d))$ where each $+$ and \times -gate is of fan-in 2.

5. Proof of Proposition 13

Let f be a homogeneous polynomial computed by a circuit \tilde{C} of size s such that

- the fan-in of each $+$ -gate is unbounded,
- the fan-in of each \times -gate is bounded by 2,
- \tilde{C} is homogeneous.

First, we can assume that all the internal vertices are of positive degree. To do that, we just have to replace recursively each gate such that all entries are of degree 0 by the constant value of this gate. Then, by homogeneity, constants cannot be entries of a $+$ -gate. Then, for each \times -gate such that one entry is a constant, we replace the \times -gate by a scalar \odot -gate. We can notice that this transformation does not increase the size of the circuit. Second, we can reorder the children of the \times -gates and of the \odot -gates such that for each one of these gates, the degree of the rightmost child is larger or equals the degree of the other child. We get a circuit C_1 of size s .

We define now a new circuit C_2 which satisfies the criteria of the proposition. For each pair of gates α and β in C_1 , we define the gate $(\alpha; \beta)$ in C_2 as follows (we will see after how to compute it):

- If β is a leaf, then $[(\alpha; \beta)]$ equals the sum of the parse trees rooted in α such that β appears in the rightmost path (i.e., the leaf of the rightmost path corresponds to the gate β).
- If β is not a leaf, then $[(\alpha; \beta)]$ equals the sum of the parse trees rooted in α such that β appears in the rightmost path and where the subtree rooted in this rightmost gate β is deleted. That is as if we replace the rightmost appearance of the gate β by the input 1 and we compute $[(\alpha; \beta)]$ with $\beta = 1$ a leaf.

We notice here that it is easy to get the polynomial computed by the gate α :

$$\begin{aligned} [\alpha] &= \sum_{T_\alpha \text{ parse tree}} \text{value}(T_\alpha) \\ &= \sum_{l \text{ leaf of } C_1} \sum_{\substack{T_\alpha \text{ parse tree s.t.} \\ \text{the rightmost leaf of } T_\alpha \\ \text{is a copy of } l}} \text{value}(T_\alpha) \\ &= \sum_{l \text{ leaf of } C_1} [(\alpha; l)]. \end{aligned}$$

We can notice that the number of parse trees can be exponential but the last sum is of polynomial size.

Now, we show how one can compute the value of the gates $(\alpha; \beta)$.

- If β does not appear on the rightmost path of a parse tree rooted in α , then $(\alpha; \beta) = 0$.
- In the case $\alpha = \beta$, if α is a leaf, then $(\alpha, \beta) = \alpha$ and else $(\alpha, \beta) = 1$.
- Otherwise α and β are two different gates and α is not a leaf. If α is a $+$ -gate, then $[(\alpha; \beta)]$ is simply the sum of all $[(\alpha'; \beta)]$, where α' is a child of α .
- If α is a \odot -gate, then one child is a constant c and the other child is a gate α' . Then $(\alpha; \beta)$ is simply the scalar operation $[(\alpha; \beta)] = [(c; c)] \odot [(\alpha'; \beta)]$.
- If α is a \times -gate. There are two cases.
 - First case: β is a leaf. Then $\deg(\alpha) > \deg(\beta)$ and $\deg(\beta) \leq 1$. On each rightmost path ending on β of a parse tree rooted in α , there exists exactly one \times -gate γ and its right child on this path γ_r such that:

$$\deg(\gamma) > \frac{1}{2} \deg(\alpha) \geq \deg(\gamma_r). \quad (1)$$

Conversely, we notice that for each gate γ satisfying (1), if $[(\alpha; \gamma)]$ and $[(\gamma_r; \beta)]$ are not zero, then γ is on a rightmost path from α to β . Then,

$$[(\alpha; \beta)] = \sum_{l \text{ leaf}, \gamma \times\text{-gate verifying (1)}} [(\alpha; \gamma)][(\gamma_l; l)][(\gamma_r; \beta)].$$

As β is a leaf, $\deg(\alpha; \beta) = \deg(\alpha)$. Using (1):

$$\deg(\alpha; \gamma) = \deg(\alpha) - \deg(\gamma) < \deg(\alpha)/2$$

$$\deg(\gamma_l; \beta) = \deg(\gamma_l) \leq \deg(\alpha)/2$$

$$\deg(\gamma_l; l) = \deg(\gamma_l) \leq \deg(\gamma_r) \leq \deg(\alpha)/2.$$

Consequently, $[(\alpha; \beta)]$ is computed by a depth-2 circuit of size at most $s^2 + 1$: a $+$ -gate, of fan-in s^2 , where each child is a \times -gate of fan-in 3. Each child of these \times -gates is of degree at most the half of the degree of the \times -gate.

– Second case: β is not a leaf. Then there exists on every rightmost paths rooted in α a \times -gate γ and its child on this path γ_r such that:

$$\deg(\gamma) \geq (\deg(\alpha) + \deg(\beta))/2 > \deg(\gamma_r). \quad (2)$$

Then by the same argument,

$$[(\alpha; \beta)] = \sum_{l \text{ leaf}, \gamma \times\text{-gate verifying (2)}} [(\alpha; \gamma)][(\gamma_l; l)][(\gamma_r; \beta)]. \quad (3)$$

We have this time with (2):

$$\deg(\alpha; \beta) = \deg(\alpha) - \deg(\beta)$$

$$\deg(\alpha; \gamma) = \deg(\alpha) - \deg(\gamma) \leq (\deg(\alpha) - \deg(\beta))/2$$

$$\deg(\gamma_r; \beta) = \deg(\gamma_r) < (\deg(\alpha) - \deg(\beta))/2.$$

The problem here is that the degree of $(\gamma_l; l)$ could be larger than $(\deg(\alpha) - \deg(\beta))/2$. The gate α is a \times -gate and its left child is of positive degree (otherwise α would be a \odot -gate). Hence, $\deg(\alpha; \beta) > \deg(\gamma_l; l)$. If γ_l is of degree at most 1 (and so exactly 1 since γ is not a \odot -gate), then $(\alpha; \beta)$ is of degree at least 2. The computation of the gate $(\alpha; \beta)$ by the formula (3) works (i.e., the degree of $(\gamma_l; l)$ is smaller than half of the degree of $(\alpha; \beta)$). Otherwise, the degree of γ_l is at least 2 and at most $\deg(\alpha; \beta)$. As l is a leaf, we can apply the first case to the gate γ_l (even if γ_l is not a \times -gate). There exists also on every rightmost paths ending on l and rooted in γ_l a \times -gate μ and its child on this path μ_r such that:

$$\deg(\mu) > \deg(\gamma_l)/2 \geq \deg(\mu_r). \quad (4)$$

Then,

$$[(\gamma_l; l)] = \sum_{\substack{l_2 \text{ leaf of } C_1 \\ \mu \times\text{-gate verifying (4)}}} [(\gamma_l; \mu)][(\mu_l; l_2)][(\mu_r; l)].$$

And so,

$$[(\alpha; \beta)] = \sum_{l, l_2, \gamma, \mu} [(\alpha; \gamma)][(\gamma_r; \beta)][(\gamma_l; \mu)][(\mu_l; l_2)][(\mu_r; l)], \quad (5)$$

where the sum is taken over all l, l_2 leaves of C_1 , γ \times -gate verifying (2) and μ \times -gate verifying (4).

The degrees of the gates $(\gamma_l; \mu)$, $(\mu_l; l_2)$ and $(\mu_r; l)$ are bounded by half of the degree of γ_l . Hence, $[(\alpha; \beta)]$ is computed by a depth-2 size- $s^4 + 1$ circuit. The \times -gates are of fan-in bounded by 5 and the degree of their children is bounded by half their degree.

Consequently, for each gates α and β in C_1 , the gate $(\alpha; \beta)$ is computed in C_2 by a sub-circuit of size at most $s^4 + 1$. At the end we get a circuit of size at most $s^6 + s^2$ which computes all gates $(\alpha; \beta)$. Finally, f is computed by a circuit of size bounded by $s^6 + s^2 + 1$.

That proves the proposition.

6. Proof of Theorem 6

For realizing the reduction to depth four, Koiran begins by transforming the circuit into an equivalent arithmetic branching program. Then, he parallelizes the branching program, and finally comes back to the circuits. The problem with this strategy is that the transformation from circuits to branching programs requires an increase in the size of our object. If the circuit is of size s , our new branching program is of size $s^{\log(d)}$. Here, the approach is to directly parallelize the circuit without using arithmetic branching programs in intermediate steps.

The idea is to split the circuit into two parts: gates of degree lower than \sqrt{d} and gates of larger degree. Furthermore, a circuit such that the degree of each gate is bounded by \sqrt{d} computes a degree- \sqrt{d} polynomial and so can be written as a sum of at most $s^{O(\sqrt{d})}$ monomials. Then, if each part of our circuit computes polynomials of degrees bounded by \sqrt{d} , we just have to get the two depth-2 circuits and connect them together. The main difficulty comes from the fact it is not always true that the sub-circuit obtained by the gates of degree larger than \sqrt{d} is of degree smaller than \sqrt{d} . For example, for the comb graph with $n - 1 \times$ -gates and n variable inputs:

$$x_1 \cdot (x_2 \cdot (x_3 \cdot (\dots)))$$

the degree of the first part is \sqrt{n} , but the degree of the second one is $n - \sqrt{n}$. In fact, we will show that this problem does not happen if we just consider \times -balanced graphs. In this case, the two parts have a degree bounded by \sqrt{d} .

Moreover, following ideas from [2], we are going to cut not exactly at level \sqrt{d} . It will give a sharper result.

Lemma 15. *Let f be a homogeneous n -variate polynomial of degree d computed by a homogeneous \times -balanced $\{\times, +, \odot\}$ -circuit C of size σ . Then f is computed by a homogeneous $\sum \prod^{[15a]} \sum \prod^{[\frac{d}{a}]}$ circuit of size $1 + \binom{\sigma+15a}{15a} + \sigma + \sigma \binom{n+\frac{d}{a}}{\frac{d}{a}} + n$ for any positive constant a smaller than d .*

To get nicer expressions, we will use the following consequence of Stirling's formula: (A proof appears in [6].)

Lemma 16.

$$\binom{k+l}{l} = 2^{O(l+l \log \frac{k}{l})}$$

First, let us see how Lemma 15 implies Theorem 6.

Proof of Theorem 6. Let f be an n -variate polynomial computed by a circuit of size s and degree d . Let \tilde{C} be the homogeneous circuit for the polynomial that we get by Proposition 10. The circuit \tilde{C} is of size $t = s(d+1)^2$ and computes all polynomials f_0, \dots, f_d where f_i is the homogeneous part of f of degree i . Then by Proposition 13, for each $i \leq d$, there exists a homogeneous \times -balanced circuit C of size $\sigma = t^6 + t^4 + 1$ computing f_i . We apply Lemma 15 for the circuit C with $a = \sqrt{d \frac{\log n}{\log \sigma}}$.

Using Lemma 16 we get a homogeneous $\sum \prod^{[O(\alpha)]} \sum \prod^{[\beta]}$ circuit of size $1 + \binom{\sigma+15a}{15a} + \sigma + \sigma \binom{n+\frac{d}{a}}{\frac{d}{a}} + n = 2^{O(\sqrt{d \log \sigma \log n})}$ with $\alpha = \sqrt{d \frac{\log n}{\log \sigma}}$ and $\beta = \sqrt{d \frac{\log \sigma}{\log n}}$. At the end, we just have to add together homogeneous parts f_i . As $\sigma = O(s^6 d^{12})$, it gives a $2^{O(\sqrt{d \log(ds) \log n})}$ upper bound for the size. \square

Proving Lemma 15 will complete the proof.

Proof of Lemma 15. We define C_1 and C_2 subcircuits of C as follows. C_1 is the subcircuit of C we get by keeping only gates of C of degree $< \frac{d}{a}$. Circuit C_2 is made up of the remaining gates (i.e., those of degree $\geq \frac{d}{a}$) and of the inputs of these gates. These inputs are the only gates which belong both in C_1 and in C_2 .

Each gate α of C_1 has degree at most $\frac{d}{a}$, so computes a polynomial of degree at most $\frac{d}{a}$. By homogeneity of C , the polynomial computed in α is homogeneous. Consequently, α is a homogeneous sum of at most $\binom{n+\frac{d}{a}}{\frac{d}{a}}$ monomials, and so, can be computed by a homogeneous depth-2 circuit of size $1 + \binom{n+\frac{d}{a}}{\frac{d}{a}} + n$. (The “1” encodes the $+$ -gate, the “ n ” encodes the input gates, and the remainder encodes the \times -gates.)

We are going to show now that the degree of C_2 is bounded by $15a$.

Let δ be the degree of C_2 . There exists a degree- δ monomial m in C_2 . Let T be a parse tree computing m .

We can notice that a gate of C_2 can occur in many parse trees, and that in a parse tree one could find several copies of a gate of C_2 .

We partition the set of \times -gates of T into 3 sets:

- $\mathcal{G}_0 = \{\alpha \in T \mid \alpha \text{ is a } \times\text{-gate and all children of } \alpha \text{ are leaves of } T\}$
- $\mathcal{G}_1 = \{\alpha \in T \mid \alpha \text{ is a } \times\text{-gate and exactly one child of } \alpha \text{ is not a leaf}\}$
- $\mathcal{G}_2 = \{\alpha \in T \mid \alpha \text{ is a } \times\text{-gate and at least two children of } \alpha \text{ are not leaves}\}.$

Then, if we consider the sub-tree S of T where the gates of S are exactly the gates of T which do not appear in C_1 , then \mathcal{G}_0 are leaves of S , \mathcal{G}_1 are internal vertices of fan-in 1 and \mathcal{G}_2 are internal vertices of fan-in at least 2.

The proof is in two parts. First we upperbound the size of the sets \mathcal{G}_0 , \mathcal{G}_1 and \mathcal{G}_2 . Then, we upperbound the degree of m .

In C , by Lemma 11, the degree of m is at least the sum of the degrees of the gates of \mathcal{G}_0 (since two of these gates cannot appear on the same path). Each one of these gates is in C_2 , so is of degree at least $\frac{d}{a}$ in C . As m is of degree at most d in C , it means that the number of gates in \mathcal{G}_0 is at most a .

In C , always by Lemma 11, the degree of m is at least the sum of the degrees of the leaves of C_2 directly connected to a gate of \mathcal{G}_1 . For each gate α of \mathcal{G}_1 , exactly one of its inputs β is in C_2 , hence of degree at least $\frac{d}{a}$ in C . By Proposition 13, the degree of α is at least two times the degree of β , it yields that the sum of degrees of inputs of α which are in C_1 is also at least $\frac{d}{a}$. Then, the number of vertices in \mathcal{G}_1 is at most a .

Finally, in a tree, the number of leaves is larger than the number of vertices of fan-in at least 2. Then in S , we get that:

$$|\mathcal{G}_2| \leq |\mathcal{G}_0| \leq a.$$

In C_2 , the degree of the monomial m is the number of leaves labelled by a non-constant leaf in T . We match each leaf with the first \times -gate which is connected to it. As in T , the fan-in of the \times -gates is bounded by 5, the fan-in of the $+$ -gates is bounded by 1 and each \odot -gates add only one constant input, then the number of variable leaves connected to a particular \times -gate is at most 5. So the number of leaves in T is at most:

$$5 \times (|\mathcal{G}_0| + |\mathcal{G}_1| + |\mathcal{G}_2|) \leq 15a.$$

This proves that the degree of C_2 is at most $15a$. Then, the number of inputs of C_2 is bounded by the number of gates in C_1 and so in C (which is σ). So, there exists a depth-2 circuit which compute C_2 , of size $1 + \binom{\sigma + 15a}{15a} + \sigma$ with as inputs the gates of C_1 .

Consequently, each polynomial f_i can be computed by a homogeneous $\sum \prod^{[a]} \sum \prod^{[\frac{d}{a}]}$ circuit of size at most $1 + \binom{\sigma + 15a}{15a} + \sigma + \sigma \binom{n + \frac{d}{a}}{\frac{d}{a}} + n$. \square

7. A lower bound

In [3], it was proved that if a homogeneous depth-four circuit computing PERM_n has its bottom fan-in bounded by t , then the size of the circuit is at least $2^{\Omega(\frac{n}{t})}$. But what happens if bottom multiplication gates all have a large fan-in? We show that this implies a similar lower bound for the size of the circuit:

Theorem 17. *If C is a homogeneous $\sum \prod \sum \prod$ circuit which computes PERM_n (or DET_n) such that the fan-in of each bottom multiplication gate is at least t , then the size of C is at least $2^{\Omega(t \log(n))}$.*

Our approach is only based on counting the number of monomials. We begin by some definitions.

Definition 18. For a multivariate polynomial $f(\mathbf{x}) = \sum_{i=1}^{m_f} a_i \mathbf{x}_i$, we will denote \mathcal{M}_f the set $\{\mathbf{x}_i \mid \mathbf{x}_i \text{ is a monomial of } f\}$. If E is a set of polynomials, we also define $\mathcal{M}_E = \bigcup_{f \in E} \mathcal{M}_f$.

We can notice $\mathcal{M}_{\text{PERM}_n} = \{x_{1,\sigma(1)} \dots x_{n,\sigma(n)} \mid \sigma \in \mathfrak{S}_n\}$. So, $|\mathcal{M}_{\text{PERM}_n}| = n!$.

Definition 19. Let E be a set of polynomials. Let us denote

$$E^+ = \{f_1 + \dots + f_m \mid m \in \mathbb{N} \text{ and } \forall i \leq m, f_i \in E\}$$

$$\text{and } E^{\times k} = \{f_1 \times \dots \times f_m \mid m \leq k \text{ and } \forall i \leq m, f_i \in E\}$$

Lemma 20. *Let E be a set of polynomials. Then,*

$$\mathcal{M}_{E^+} = \mathcal{M}_E \quad \text{and} \quad |\mathcal{M}_{E^{\times 5}}| \leq (|\mathcal{M}_E| + 1)^5.$$

Proof. If \mathbf{x} is a monomial in \mathcal{M}_{E^+} , it means there exist polynomials f_1, \dots, f_m in E such that \mathbf{x} is a monomial of $f_1 + \dots + f_m$. Then there exists $i \leq m$ such that \mathbf{x} is a monomial of f_i and so \mathbf{x} is an element of \mathcal{M}_E . Hence $\mathcal{M}_{E^+} \subseteq \mathcal{M}_E$. Moreover, as $E \subseteq E^+$, we get $\mathcal{M}_E \subseteq \mathcal{M}_{E^+}$.

Moreover, if \mathbf{x} is a monomial in $\mathcal{M}_{E \times s}$, it means there exist polynomials f_1, \dots, f_m in E such that \mathbf{x} is a monomial of $f_1 \times \dots \times f_m$ with $m \leq s$. It implies that $\mathbf{x} \in \{\mathbf{x}_1 \times \dots \times \mathbf{x}_m \mid m \leq s \text{ and } \mathbf{x}_i \in \mathcal{M}_E\}$. That is to say, $\mathbf{x} \in \{\mathbf{x}_1 \times \dots \times \mathbf{x}_s \mid \mathbf{x}_i \in (\mathcal{M}_E \cup \{1\})\}$. It proves the lemma. \square

Let C be a $\sum \prod \sum \prod$ circuit. The gates of the circuit are layered into five levels. Inputs are at level 0, multiplication gates at levels 1 and 3 and addition gates at levels 2 and 4. For each level i , let us denote s_i the number of gates at this level, t_i an upper bound on the fan-in of these gates and E_i the set of polynomials computed at this level.

Lemma 21. Any $\sum \prod \sum \prod$ circuit that computes PERM_n (or DET_n) such that the fan-in of the multiplication gates at level 3 is bounded by v must have size $\exp[\Omega(\frac{n}{v} \log(n))]$.

Proof. We notice that the hypothesis in the lemma about the bound of the fan-in just states that $t_3 \leq v$.

The polynomials in E_1 are just monomials. So, $|\mathcal{M}_{E_1}| \leq s_1$. We have:

$$E_4 \subseteq E_3^+, \quad E_3 \subseteq E_2^{\times t_3} \quad \text{and} \quad E_2 \subseteq E_1^+.$$

Then by Lemma 20,

$$|\mathcal{M}_{E_4}| \leq (s_1 + 1)^{t_3} \leq (s_1 + 1)^v.$$

However, as PERM_n is an element of E_4 , we also have:

$$|\mathcal{M}_{E_4}| \geq |\mathcal{M}_{\text{PERM}_n}| = n!.$$

So, $s_1 \geq (n!)^{\frac{1}{v}} - 1 = 2^{\Omega(\frac{n}{v} \log(n))}$. \square

The result of this lemma directly implies Theorem 17.

Proof of Theorem 17. Let C be a homogeneous $\sum \prod \sum \prod$ circuit which computes PERM_n (or DET_n) such that the fan-in of each bottom gate is at least t . It implies that the degree of each gate at level 1 and 2 is at least t . As the circuit is homogeneous, the degree of a gate at level 3 is upperbounded by n and lowerbounded by t times the number of inputs of this gate. Consequently, in C , the fan-in of the multiplication gates at level 3 is bounded by $\frac{n}{t}$. Then Lemma 21 implies the theorem. \square

In fact, for computing the determinant, we can also notice that the fan-in of multiplication gates in the depth-four circuits that we get either in [1] or here in Section 6, is linear in \sqrt{n} . It implies that in this case, the bounds are tight.

Corollary 22. If C is a $\sum \prod \sum \prod$ circuit which computes DET_n such that the fan-in of each bottom multiplication gate is $\Omega(\sqrt{n})$ or such that the fan-in of each multiplication gate of level 3 is $O(\sqrt{n})$, then the minimal size of C is $2^{\Theta(\sqrt{n} \log(n))}$.

Proof. Koiran's result [1] implies that there exist depth-four circuits for DET_n of size $2^{O(\sqrt{n} \log n)}$ such that all multiplication gates have fan-in bounded by $O(\sqrt{n})$. For the lowerbound, the case where the bottom fan-in is lowerbounded by $\Omega(\sqrt{n})$ is given by Theorem 17. The case where the fan-in of gates of level 3 is bounded by $O(\sqrt{n})$ is given by Lemma 21. \square

It would be interesting to know the lower bound on the size of a homogeneous circuit computing DET_n . In [3] the authors show that if the circuit is such that the fan-in of bottom gates is bounded by $O(\sqrt{n})$, then the size is $2^{\sqrt{n}}$. Here, we show that if all bottom fan-in are lowerbounded by $\Omega(\sqrt{n})$, then the size is $2^{\Omega(\sqrt{n} \log n)}$. What happens if in the circuit, there are some bottom gates with a large fan-in and some bottom gates with a small fan-in?

Open question. Is it true that if C is a homogeneous depth-four circuit which computes DET_n then the size of C is at least $2^{\Omega(\sqrt{n})}$?

Acknowledgments

The author thanks Pascal Koiran for helpful discussions and comments on this work.

References

- [1] P. Koiran, Arithmetic circuits: the chasm at depth four gets wider, Theor. Comput. Sci. 448 (0) (2012) 56–65, <http://dx.doi.org/10.1016/j.tcs.2012.03.041>, <http://www.sciencedirect.com/science/article/pii/S0304397512003131>.
- [2] A. Gupta, P. Kamath, N. Kayal, R. Saptharishi, Arithmetic circuits: a chasm at depth three, Electron. Colloq. Comput. Complex., <http://dx.doi.org/10.1109/FOCS.2013.68>.

- [3] A. Gupta, P. Kamath, N. Kayal, R. Saptharishi, Approaching the chasm at depth four, in: *Proceedings of the Conference on Computational Complexity (CCC)*, <http://dx.doi.org/10.1109/CCC.2013.16>.
- [4] L. Valiant, S. Skyum, S. Berkowitz, C. Rackoff, Fast parallel computation of polynomials using few processors, *SIAM J. Comput.* 12 (4) (1983) 641–644, <http://dx.doi.org/10.1137/0212043>.
- [5] E. Allender, J. Jiao, M. Mahajan, V. Vinay, Non-commutative arithmetic circuits: depth reduction and size lower bounds, *Theor. Comput. Sci.* 209 (1–2) (1998) 47–86, [http://dx.doi.org/10.1016/S0304-3975\(97\)00227-2](http://dx.doi.org/10.1016/S0304-3975(97)00227-2).
- [6] M. Agrawal, V. Vinay, Arithmetic circuits: a chasm at depth four, in: *Proceedings-Annual Symposium on Foundations of Computer Science, 2008*, pp. 67–75.
- [7] H. Fournier, N. Limaye, G. Malod, S. Srinivasan, Lower bounds for depth 4 formulas computing iterated matrix multiplication, *Electron. Colloq. Comput. Complex.* 20 (2013) 100.
- [8] J. von zur Gathen, Feasible arithmetic computations: Valiant's hypothesis, *J. Symb. Comput.* 4 (2) (1987) 137–172, [http://dx.doi.org/10.1016/S0747-7171\(87\)80063-9](http://dx.doi.org/10.1016/S0747-7171(87)80063-9).
- [9] P. Bürgisser, *Completeness and Reduction in Algebraic Complexity Theory*, *Algorithms Comput. Math.*, vol. 7, Springer, 2000.
- [10] A. Shpilka, A. Yehudayoff, Arithmetic circuits: a survey of recent results and open questions, *Found. Trends Theor. Comput. Sci.* 5 (3–4) (2009), <http://dx.doi.org/10.1561/04000000039>.
- [11] X. Chen, N. Kayal, A. Wigderson, Partial derivatives in arithmetic complexity and beyond, *Found. Trends Theor. Comput. Sci.* (2011).
- [12] G. Malod, N. Portier, Characterizing Valiant's algebraic complexity classes, *J. Complex.* 24 (1) (2008) 16–38.