Electronic Colloquium on Computational Complexity, Report No. 42 (1998)

ECCC

A Note On the Use of Determinant for Proving Lower Bounds on the Size of Linear Circuits

Pavel Pudlák *

July 2, 1998

Abstract

We consider computations of linear forms over $\mathbf{R}$ by circuits with linear gates where the absolute values coefficients are bounded by a constant. Also we consider a related concept of restricted rigidity of a matrix. We prove some lower bounds on the size of such circuits and the restricted rigidity of matrices in terms of the absolute value of the determinant of the matrix.

1

The purpose of this note is to analyze the role of the determinant in establishing lower bounds for linear circuits over $\mathbf{R}$ with bounds on the coefficients. The study of the linear complexity of computation has a long history, starting with the seminal works of Morgenstern [6, 7], Grigoriev [4] and Valiant [10]. But it is still an open problem to prove more than linear lower bounds on general circuits computing an explicitly defined linear form. With the restriction on the size of coefficients, Morgenstern [7] proved nontrivial lower bounds on the size of linear circuits. He showed that the number of additions and scalar multiplications in a fan-in 2 circuit for computing linear forms associated with a matrix A is at least $\log_c |Det(A)|$, with c being the maximum of the sum of the absolute values of the coefficients used in any linear combination. He was thus able to prove, e.g., an $\frac{1}{2}n \log_2 n$ lower bound for the circuit size of an $n \times n$ DFT, under the restriction that $c \leq 2$. This method, unfortunately, does not work for unrestricted computations, since we get the same bound, say, for nI, where I is the $n \times n$ identity matrix, but it is not excluded that it can be somehow modified to more general models of computation.

Several researchers further analyzed the complexity of computing linear forms in the restricted linear model, using the singular values of the matrix

*Mathematical Institute, AVČR, Žitná 25, 115 67 Praha 1, Czech Republic. e-mail: pudlak@math.cas.cz, Supported by grant no. A1019602 of the Academy of Sciences of the Czech Republic, and grant INT-9600919/ME 103(1997) under the cooperation of MŠMT, Czech Republic and NSF, USA. Main part of this work was done while visiting Istituto di Matematica Computazionale del CNR, Pisa, Italy.

ISSN 1433-8092

and Wielandt-Hoffman inequality (Nisan and Wigderson [8], Chazelle [3], Lokam [5]).

In this paper we will show that several such results can also be obtained using bounds on the determinants. Our main tool will be Hadamard's inequality (see eg. [1]) for the determinant of a complex valued matrix, which states that

$$|Det(A)| \leq \prod_{j=1}^{n} \sqrt{\sum_{i=1}^{n} |a_{ij}|^2}. \tag{1}$$

Several previous results follow from ours, with only slightly worse constants, which shows that the "volume argument" can be used in most cases for such lower bounds.

In particular we show that matrices with large determinant have large restricted rigidity, and that linear circuit with coefficients by c of depth d for the computation of linear forms associated with a matrix with large determinant must have size at least $dn^{1+\frac{1}{d}}/c^2$.

Our lower bound techniques apply to matrices A such that $\log_c |Det(A)|$ is nonlinear, e.g., $n \log n$. Example of such matrices, with constant entries, are the Fourier matrix, the Hadamard matrix, as well as the Jacobsthal circulant matrix, i.e., the matrix whose (i,j)-th entry is given by $\chi(i-j)$, where χ is the Legendre symbol.

2

In what follows, $||A||_F$ will denote the Frobenius norm of a matrix A, i.e. the square root of the sum of the squares of its entries. We will make use of the following upper bound on the determinant:

$$Det(A) \leq \left(\frac{||A||_F^2}{n} \right)^{n/2}, \tag{2}$$

which follows from Hadamard inequality using the inequality between geometric and arithmetic means. Let us note that this bound is sharp for Fourier and Hadamard matrices, since the absolute value of their determinant is equal to $n^{n/2}$, and that, by adding a rank one matrix to the Jacobsthal matrix, one also obtains a matrix whose determinant is $n^{n/2}$.

This bound can be extended to the product of rectangular matrices as follows.

Lemma 1 *Let an $n \times n$ matrix A be the product of k rectangular matrices $A_1, A_2, \ldots, A_k$, then*

$$|Det(A)| \leq \left(\frac{||A_1||_F^2}{n} \right)^{n/2} \left(\frac{||A_2||_F^2}{n} \right)^{n/2} \cdots \left(\frac{||A_k||_F^2}{n} \right)^{n/2}.$$

Proof. We prove it by induction on k. The basis is inequality (2). Suppose the statement holds for $k-1$, and consider a product of k matrices. Let A_1 be an $n \times m$ matrix. We can assume that $m \geq n$, otherwise A is singular. Let K be an orthogonal $m \times m$ matrix which maps the rows of A_1 onto vectors with all coordinates i, $n < i \leq m$, equal to zero. There is such a matrix, since the dimension of the space spanned by the rows is at most n. Write the product as follows:

$$A_1 K K^{-1} A_2 A_3 \dots A_k.$$

Let A_1' be $A_1 K$ with the last $m-n$ columns omitted and let A_2' be $K^{-1}A_2$ with last $m-n$ rows omitted. Clearly $A = A_1' A_2' A_3 \dots A_k$. Since A_1 is a square matrix, and applying the induction hypothesis, we get

$$|Det(A)| = |Det(A_1')||Det(A_2' A_3 \dots A_k)| \leq$$

$$\left(\frac{||A_1'||_F^2}{n}\right)^{n/2} \left(\frac{||A_2'||_F^2}{n}\right)^{n/2} \left(\frac{||A_3||_F^2}{n}\right)^{n/2} \dots \left(\frac{||A_k||_F^2}{n}\right)^{n/2}.$$

It remains to observe that $||A_1'||_F^2 = ||A_1||_F^2$ and $||A_2'||_F^2 \leq ||K^{-1}A_2||_F^2 = ||A_2||_F^2$. □

First we consider a bound to rigidity with restriction on the size of entries involved. We denote by $R_A(r,c)$, the *restricted rigidity* of A, the minimal number of nonzero entries in a matrix C such that A can be written as $A = B + C$, where B is a rank r matrix, and the absolute values of all the entries of B and C do not exceed c.

Theorem 1 *Let A be an $n \times n$ matrix with entries of absolute value $\leq c$, for some constant $c \geq 1$; let $r \leq n/2$. Then*

$$R_A(r,c) \geq (n-r)\left(\frac{|Det(A)|}{r^{r/2}}\right)^{\frac{2}{n-r}} c^{-O(1)}.$$

Proof. Let $A = B + C$, where B is a rank r matrix. A well known property of the determinant allows us to express the determinant of A in terms of determinants of submatrices of B and C. Thus we obtain

$$|Det(A)| \leq \sum_{k=1}^{r} \sum_{B_k, C_{n-k}} |Det(B_k)||Det(C_{n-k})| \leq$$

$$\sum_{k=1}^{r} \binom{n}{k}^2 \max_{B_k, C_{n-k}} |Det(B_k)||Det(C_{n-k})|$$

where B_k ranges $k \times k$ submatrix of B, and C_{n-k} is the $(n-k) \times (n-k)$ submatrix of C, with rows and columns disjoint from those of B_k. Using the inequality (2) we upper bound $|Det(B_k)|$ by $\left(\frac{c^2 k^2}{k}\right)^{k/2} = c^k k^{k/2}$, and

$|Det(C_{n-k})|$ by $(\frac{c^2R}{n-k})^{\frac{n-k}{2}}$. We can also upper bound $\sum_{k=1}^{r}\binom{n}{k}^2$ by 4^n. Thus we obtain

$$|Det(A)| \leq \frac{c^k k^{k/2}}{4^n}\left(\frac{c^2R}{n-k}\right)^{\frac{n-k}{2}},$$

for a certain value of $k \leq r$, from which

$$R \geq \frac{(n-k)|Det(A)|^{\frac{2}{n-k}}}{c^2\left(4^n c^k k^{k/2}\right)^{\frac{2}{n-k}}}.$$

To find the minimum of the expression is tedious but a routine application of elementary calculus. First we find that the second derivative with respect to k is positive in the range that we are interested in. Thus it attains minimum either for $k = 1$ or $k = r$. It turns out that the value for $k = 1$ can be smaller than value for $k = r$ by at most a power of c, thus we get the lower bound of the theorem.

We leave the details of the computation to the reader. □

Corollary 1 *Let A be an $n \times n$ matrix such that $|Det(A)| = n^{n/2}$. Then, for $r \leq n/2$,*

$$R_A(r, c) = c^{-O(1)}n(n-r).$$

Proof.

$$\left(\frac{|Det(A)|}{r^{r/2}}\right)^{\frac{2}{n-r}} = \left(\frac{n^n}{r^r}\right)^{\frac{1}{n-r}} \geq \left(\frac{n^n}{(n/2)^r}\right)^{\frac{1}{n-r}} = n2^{\frac{r}{n-r}} \geq n2^{\frac{n/2}{n-n/2}} = 2n.$$

□

Next we shall consider linear circuits of unbounded fan-in. This means that a gate in a circuit computes a linear function of inputs and the number of inputs to the gate can be arbitrary (not just one or two). The natural measure of complexity is then not the number of gates (since, trivially, we would need only the output gates) but *the number of edges* of the graph of the circuit, also called *the number of wires*. The classical model, used, e.g., by Morgenstern, counts the number of scalar multiplications and additions. This is up to a multiplicative constant the same as counting the number of wires in fan-in two circuits. Let us stress, however, that these measures do not coincide even in this case. Namely, a value obtained in one addition gate may be sent directly to another addition gate, or may be multiplied by a scalar before that. This gives 0 resp. 1 operation, while if we count the edges of the graph, we always count it as 1.

Now we prove a lower bound on the minimum size of depth d circuits. Our model of depth restricted circuits is *synchronous*, which means that all paths from inputs to an output gate have the same length. Thus the computation can be represented as a product of matrices, where matrices correspond to transformations from a given layer to the next.

Theorem 2 *The number of edges S of a depth d linear circuit for computing linear forms associated to an $n \times n$ matrix A satisfies $S \geq dn|Det(A)|^{\frac{2}{dn}}/c^2$, where c is the maximal absolute value of the coefficients used in the circuit. In particular, if A is the Fourier or a Hadamard matrix we have $S \geq dn^{1+\frac{1}{d}}/c^2$.*

Proof. The computation of linear forms associated to an $n \times n$ matrix A by a depth d circuit corresponds to a factorization of A into the product of d rectangular matrices $A_1, A_2, \ldots, A_d$. Now we use the inequality (2) from which we can derive, by applying the inequality between arithmetic and geometric mean,

$$|Det(A)| \leq \left(\frac{\sum_{i=1}^{d} ||A_i||_F^2}{nd} \right)^{\frac{dn}{2}}. \tag{3}$$

The thesis then readily follows from the fact that $\sum_{i=1}^{d} ||A_i||_F^2 \leq c^2 S$, where S is the number of edges in the circuit. □

Let us note that in the above theorem we actually do not bound the number of wires, but the the euclidean norm of the vector of coefficients and then we use the information on the maximal size of coefficients to estimate the size of the circuit. Similarly in Theorem 1 we just bound the Frobenius norm instead of the number of nonzero elements. The bound of Morgenstern [6] mentioned above seems very similar, but it does not seem to be possible to interpret it in such a way, since the bound is proportional to the inverse of $\log c$, rather than to the inverse of c^2 as in our bounds.

By minimizing the lower bound over all depths we get the following result from the theorem above.

Corollary 2 *The minimal size of a synchronous circuit with coefficients of absolute value $\leq c$ computing the linear transformation given by a complex matrix A is at least $2e \ln |Det(A)|/c^2$.*

Let us fix $c = 1$. For $n \times n$ Fourier and Hadamard matrices we thus get a lower bound $\frac{en \ln n}{c^2} \approx 1.88 n \log_2 n$ on the number of wires. If all the coefficients had absolute value 1, the gates would need to have fan-in equal to e, which is not an integer. If we count, however, the minimal number of wires in circuits of fan-in three we get only a slightly bigger constant ≈ 1.89. For fan-in 2 we get $2n \log n$, which matches the upper bound given by the Cooley-Tuckey algorithm. Unfortunately we can prove this only under the restriction that the synchronous circuit computing a $n \times n$ matrix has *width* n.

Here is the computation. Under the restriction mentioned above, such a circuit can be represented as a product of $n \times n$ matrices. Now we use the Hadamard inequality (1). Observe that the terms in the product are just the euclidean norms of the vectors of coefficients of edges directed to a gate. Assume that each gate has fan-in either 1 or k. Then the norm of the vector of coefficients of a gate of fan in 1, resp. k is bounded by 1 resp. $\sqrt{k}$.

Thus we get a bound $k^{\frac{S}{2}} \geq |Det(A)|$, for the number S of gates of fan-in k, which gives the above bounds. Note that we do not count the fan-in 1 gates, so we, in some sense, are dealing with nonsynchronous circuits, but due to the restriction on the width of the circuit, the class of circuits to which it applies is still very restricted.

This computation shows that the Hadamard inequality gives us additional information that other tools used in this area have not been able to capture. We can deduce that in an optimal circuit (with all the restriction that we are considering) the fan-ins must be essentially equal. Applying the inequality to the transposed matrices, we get the same for fan-outs.

Acknowledgment

I would like to thank to Bruno Codenotti for many fruitful discussions.

References

[1] R. Bellman, *Introduction to Matrix Analysis*, 2nd Ed. McGraw Hill, New York (1970).

[2] P. Bürgisser, M. Clausen, M. A. Shokrolahi, *Algebraic Complexity Theory*, Springer 1997.

[3] B. Chazelle, *A Spectral Approach to Lower Bounds*, Proc. 35th IEEE FOCS (1994), 674-682.

[4] D. Yu. Grigoriev, *Using the notion of separability and independence for proving lower bounds on circuit complexity*, Notes of the Leningrad branch of the Steklov Mathematical Institute, 60, (1976) 38-48.

[5] S.V. Lokam, *Spectral Methods for Matrix Rigidity with applications to size-depth Tradeoffs and Communication Complexity*, Proc. 36th IEEE FOCS (1995), 6-15.

[6] J. Morgenstern, *Note on a Lower Bound on the Linear Complexity of the Fast Fourier Transform*, J. ACM 20(2) (1973), 305-306.

[7] J. Morgenstern, *The Linear Complexity of Computation*, J. ACM 22(2) (1975), 184-194.

[8] N. Nisan and A. Wigderson, *On the Complexity of Bilinear Forms*, Proc. 27th ACM STOC (1995), 723-732.

[9] B.S. Kashin and A.A. Razborov, *Improved Lower Bounds on the Rigidity of Hadamard matrices*, preprint.

[10] L.G. Valiant, *Graph-theoretic arguments in low level complexity,* Proc. 6th MFCS, Springer-Verlag LNCS 53 (1977), 162-176.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'