A linear lower bound for the size of threshold circuits

HANS DIETMAR GRÖGER[1] AND GY. TURÁN[2,3]

There is a large number of lower bound results for unbounded fan-in Boolean circuits (see e.g. the surveys of Boppana and Sipser [2] and Wegener [11]). In most of these results the depth of the circuits is assumed to be bounded by some constant.

A linear lower bound for the size of unbounded fan-in, unbounded depth circuits, where each gate computes a commutative and associative function, was given by Hromkovic [5]. Smolensky [9] proves an $\Omega(n/\log n)$ lower bound for unbounded fan-in, unbounded depth circuits of gates computing arbitrary symmetric functions. Wegener [11] shows that unbounded depth threshold circuits computing the parity of n bits have size $\Omega(\log n)$. The Shannon function of unbounded depth threshold circuits was determined by Nechiporuk [7] and Lupanov [6].

In this note we also consider the class of unbounded depth threshold circuits and we prove a simple linear lower bound. The circuits consist of threshold gates of the form $T_k^\gamma(z_1, \ldots, z_m)$, where $\gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbf{Z}^m$, $k \in \mathbf{Z}$. The output of such a gate is 1 if $\sum_{i=1}^{m} \gamma_i z_i \geq k$, and it is 0 otherwise. The size of a circuit is the number of its gates.

No restriction is imposed on the size of the weights and on the depth of the circuit.

INNER PRODUCT MOD 2_n is the $2n$-variable function $\mathbf{x} \cdot \mathbf{y} := (x_1 \wedge y_1) \oplus \ldots \oplus (x_n \wedge y_n)$, considered e.g. in Babai, Frankl and Simon [1], Hajnal, Maass, Szegedy, Pudlák and Turán [4].

Theorem. *The size of every threshold circuit computing INNER PRODUCT MOD 2_n is at least $\frac{n}{2}$.*

Proof. We use a variant of the gate elimination method (see e.g. Wegener [10]), where gates are eliminated by restricting the set of input vectors considered. First it is observed that every threshold gate is constant on some large subrectangle of an arbitrary rectangle.

Let $T_k^\gamma(x_1, \ldots, x_n, y_1, \ldots, y_n)$ be a threshold gate with inputs $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$, where $\boldsymbol{\gamma} = (\alpha, \beta)$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, evaluating $\sum_{i=1}^{n} \alpha_i x_i + \sum_{i=1}^{n} \beta_i y_i \geq k$.

[1]Dept. of Mathematics, Berzsenyi Dániel Teachers' College, 9700 Szombathely, Károli G. tér 4, Hungary. Partially supported by OTKA F-4204.

[2]Automata Theory Research Group of the Hungarian Academy of Sciences, 6720 Szeged, Aradi tér 1, Hungary. Partially supported by OTKA 501.

[3]Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, MC/249, Box 4348, Chicago, Il. 60680, USA.

Lemma 1. *For every $X, Y \subseteq \{0,1\}^n$ there are sets $X' \subseteq X$ and $Y' \subseteq Y$ such that $|X'| \geq \frac{|X|}{2}$, $|Y'| \geq \frac{|Y|}{2}$ and T_k^γ is constant on $X' \times Y'$.*

Proof. Order the elements of X (resp. Y) according to the value of $\sum_{i=1}^{n} \alpha_i x_i$ (resp. $\sum_{i=1}^{n} \beta_i y_i$), resolving ties arbitrarily. Let $\mathbf{x}$ (resp. $\mathbf{y}$) be the element of rank $\left\lceil \frac{|X|}{2} \right\rceil$ (resp. $\left\lceil \frac{|Y|}{2} \right\rceil$) in this ordering and let X^* (resp. Y^*) be the set of elements smaller than $\mathbf{x}$ (resp. $\mathbf{y}$). If T_k^γ accepts (resp. rejects) $(\mathbf{x}, \mathbf{y})$, then $X' := X \backslash X^*$, $Y' := Y \backslash Y^*$ (resp. $X' := X^* \cup \{\mathbf{x}\}$, $Y' := Y^* \cup \{\mathbf{y}\}$) satisfy the requirements of the lemma. □

We also need the following result.

Lemma 2. (Lindsey, see e.g. [1].) *For every $X, Y \subseteq \{0,1\}^n$*

$$\Big| |\{(\mathbf{x},\mathbf{y}) \in X \times Y : \mathbf{x} \cdot \mathbf{y} = 1\}| - |\{(\mathbf{x},\mathbf{y}) \in X \times Y : \mathbf{x} \cdot \mathbf{y} = 0\}| \Big| \leq \sqrt{|X|\,|Y| 2^n}. \quad \Box$$

Thus, in particular, if INNER PRODUCT MOD 2_n is constant on $X \times Y$ with $|X| = |Y|$, then it must be the case that $|X|\,|Y| \leq \sqrt{|X|\,|Y| 2^n}$, i.e. $|X| = |Y| \leq 2^{n/2}$.

Now in order to apply gate elimination, let us consider an arbitrary threshold circuit C computing INNER PRODUCT MOD 2_n, with gates $T_1, T_2, \ldots$ given in some topological ordering. It may be assumed w.l.o.g. that the inputs of T_i are $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ and the outputs of $T_1, \ldots, T_{i-1}$, by adding edges of weight 0 if necessary.

We construct sets $X_i, Y_i \subseteq \{0,1\}^n$ with $|X_i| = |Y_i| \geq 2^{n-i}$ for $i \leq \lceil \frac{n}{2} \rceil$, such that eliminating $T_1, \ldots, T_i$ from C and possibly modifying the thresholds of the remaining gates we get a circuit that computes INNER PRODUCT MOD 2_n on $X_i \times Y_i$.

This follows by induction on i. For $i = 0$ let $X_0 = Y_0 := \{0,1\}^n$. Then X_1 and Y_1 are obtained by applying Lemma 1 to X_0, Y_0 and T_1. Restricting the set of input vectors considered to $X_1 \times Y_1$, the gate T_1 can be deleted. If the output of T_1 on $X_1 \times Y_1$ is constant 1, then after deleting T_1 the threshold of T_2 has to be decreased by the weight of the edge connecting T_1 to T_2. In general, X_i and Y_i are obtained similarly by applying Lemma 1 to X_{i-1}, Y_{i-1} and T_i.

As it holds that $|X_i| = |Y_i| \geq 2^{n-i}$, the consequence of Lemma 2 mentioned above implies that as long as $i < \frac{n}{2}$, INNER PRODUCT MOD 2_n is not constant on $X_i \times Y_i$. Hence after deleting $T_1, \ldots, T_i$ not all the gates of C are eliminated yet. This implies the claimed lower bound. □

We note that generalizing this argument one can also prove lower bounds for linear decision trees computing INNER PRODUCT MOD 2_n even if randomization with two-way errors is allowed [3]. Recently Roychowdhury, Siu and Orlitsky [8] generalized the results of Smolensky [9] and the lower bound of this note in the framework of communication complexity.

REFERENCES

[1] L. BABAI, P. FRANKL, J. SIMON: Complexity classes in communication complexity, 27 FOCS (1986), 337–347.

[2] R. BOPPANA, M. SIPSER: The complexity of finite functions, Handbook of Theoretical Computer Science (J. van Leeuwen ed.), Elsevier, 1990, 758–804.

[3] H. D. GRÖGER, GY. TURÁN: On linear decision trees computing Boolean functions, 18 ICALP (J. L. Albert, B. Monien, M. R. Artalejo eds.), LNCS 510 (1991), 707–718.

[4] A. HAJNAL, W. MAASS, P. PUDLÁK, M. SZEGEDY, GY. TURÁN: Threshold circuits of bounded depth, 28 FOCS (1987), 99–110.

[5] J. HROMKOVIC: Linear lower bounds on unbounded fan-in Boolean circuits, *Inf. Proc. Lett.* **21** (1985), 71–74.

[6] O. B. LUPANOV: Circuits using threshold elements. *Dokl. Ak. Nauk USSR* **202** (1972), 1286–1291 (in Russian). English translation: *Sov. Phys. Dokl.* **17** (1972), No. 2, 91–93.

[7] E. I. NECHIPORUK: The synthesis of networks from threshold elements, *Probl. Kib.* **11** (1964), 49–62 (in Russian). English translation: *Autom. Expr.* **7** (1964), No. 1, 35–39; No. 2, 27–32.

[8] V. P. ROYCHOWDHURY, K. Y. SIU, A. ORLITSKY: Lower bounds on threshold and related circuits via communication complexity, Technical Report TR-EE 92–29, Purdue Univ., Sch. of El. Eng., July 1992.

[9] R. SMOLENSKY: On interpolation by analytic functions with special properties and some weak lower bounds on the size of circuits with symmetric gates, 31 FOCS (1990), 628–631.

[10] I. WEGENER: The complexity of Boolean functions, Teubner–Wiley, 1987.

[11] I. WEGENER: Unbounded fan-in circuits, Univ. Dortmund, Abt. Inf., Report **267** (1988), to appear in: Advances in the Theory of Computation and Computational Mathematics, Vol. I. (L. Keener, ed.), Ablex.