An O(n log n) lower bound for the synchronous circuit size of integer multiplication

by

Kurt Mehlhorn

Fachbereich Angewandte
Mathematik und Informatik
Universität des Saarlandes
D-6600 Saarbrücken

Juli 1976

A 76/06

We prove an $O(n \log n)$ lower bound for the synchronous circuit size of integer multiplication. A circuit is synchronous, if no races occur in this circuit, or more formally, if for all gates g the following holds: all pathsfrom inputs to gate g have identical length. Here we assume that each gate introduces one time unit of delay. A circuit can always be made synchronous by introducing additional gates (delay elements). However, it is conceivable that this squares the size of the circuit. Nevertheless, from the point of view of physics, requiring a circuit to be synchronous is a very reasonable restriction.

Let $f: \{0,1\}^n \to \{0,1\}^m$ be a boolean function with n inputs and m outputs. We denote by $C^S(f)$ the size (number of gates) of the smallest synchronous circuit over the basis of all two-input gates which realizes f.

Integer multiplication is the following boolean function $\text{Mult}_n : \{0,1\}^{2n} \to \{0,1\}^{2n}$. It takes two n bit binary numbers as inputs —— $x_{2n} \ldots x_{n+1}$ and $x_n \ldots x_1$ (least significant bit to the right) —— and produces the binary representation of the product of these two numbers.

<u>Theorem:</u> $C^S(\text{Mult}_n) \geq O(n \log n)$

We prove this lower bound by appealing to results of Harper and Harper & Savage.

<u>Definition:</u> The class of functions $P^{n,m}_{p,q}(\varepsilon)$, $0 \leq \varepsilon < 1$, is defined as

$P^{n,m}_{p,q}(\varepsilon) = \{f: \{0,1\}^n \to \{0,1\}^m$; for all but a fraction ε of the subsets $I \subseteq \{1,\ldots,n\}$, $|I| = p$, the set of of n-p variables obtained by fixing the variables in I in all possible 2^p ways contains at least q different functions .

<u>Fact</u> (Harper & Savage) : Let $f \in P_{p,q}^{(n,m)}(\varepsilon)$.

Then

$$C^S(f) \geq (1-\varepsilon)\left[L - \frac{4(n-p)(2^L-1)}{p-2^L}\right]\log q$$

for every L with $0 \leq L \leq \max\left\{l;\ 2^l < p \text{ and } (1-\varepsilon)\cdot\left[1 - \frac{2(n-p)2^l}{p-2^l}\right]\log_2 q \geq m\right\}$

This result is not directly applicable to integer multiplication. Certainly, $q \leq 2^p$ and hence $\log q \leq p \leq n$. In our case $n = m$ and hence $L \leq 0$. We conclude that the result of Harper and Savage is applicable only in the case that $n > m$. Therefore we consider instead of Mult_n the following boolean function $\overline{\text{Mult}}_n : \{0,1\}^{2n} \to \{0,1\}^n$ defined as: $\overline{\text{Mult}}_n(x_{2n}\ldots x_{n+1}\ x_n\ldots x_1)$ are the n least significant bits of the binary representation of the product of the two binary numbers represented by $x_{2n}\ldots x_{n+1}$ and $x_n\ldots x_1$. Certainly

$$C^S(\text{Mult}_n) \geq C^S(\overline{\text{Mult}}_n)$$

We show that $\overline{\text{Mult}}_n \in P_{p,q}^{(2n,n)}(0.1)$ where $p = 2n - \log n$, $\log q = 3n/2 - \log n$ and n sufficiently large.

Application of Harper's and Savage's result yields:

$$\max\{l;\ 0.9.\ [1 - \frac{2\log n\ 2^l}{2n-\log n - 2^l}]\log q \geq n\}$$

$$\geq \max\{l;\ \frac{45}{40}\ [1 - \frac{2\log n\ 2^l}{2n-\log n - 2^l}]\ n \geq n\}$$

since $3n/2 - \log n \geq 5/4\ n$ for n sufficiently large

$$= \max\{l;\ \frac{2\log n\ 2^l}{2n - \log n - 2^l} \leq \frac{5}{45} = 1/9\}$$

$$= \max\{l;\ (18\log n + 1)\cdot 2^l \leq 2n - \log n\}$$

$$= \max \{l;\ l \le \log (2n - \log n) - \log (18 \log n + 1)\}$$

$$\ge 1/2 \ \log n \quad \text{for } n \text{ sufficiently large}$$

and hence

$$c^S (\overline{\mathrm{Mult}_n}) \ge 0.9 \cdot [1/2 \log n - \frac{4 \log n(\sqrt{n}-1)}{2n-\log n - \sqrt{n}}](3n/2-\log n)$$

$$\ge 0.9 \cdot 1/4 \log n \cdot n$$

$$\ge 1/5 \cdot n \cdot \log n$$

for sufficiently large n. It remains to show that $\overline{\mathrm{Mult}_n} \in P_{p,q}^{(2n,n)}$ (0.1) for $p = 2n - \log n$, $\log q = 3/2\ n - \log n$ and n sufficiently large.

Lemma 1: The fraction of the subsets $I \subsetneq \{1,\dots,2n\}$, $|I| = p$ with $\{1,\dots,n/4\} \subset I$ or $\{n+1,\dots,5n/4\} \subsetneq I$ is less than 0.1 for sufficiently large n.

Proof: I^c, the complement of I, is a subset of $\{1,\dots,2n\}$ of size log n. The condition above is equivalent to $I^c \cap \{1,\dots,n/4\} = \emptyset$ or $I^c \cap \{n + 1,\dots,5n/4\} = \emptyset$. The number of I's with $I^c \cap \{1,\dots,n/4\} = \emptyset$ is equal to $\binom{7n/4}{\log n}$ and hence the number of I's with $I^c \cap \{1,\dots,n/4\} = \emptyset$ or $I^c \cap \{n+1,\dots,5n/4\} = \emptyset$ is less than $2\cdot\binom{7n/4}{\log n}$. Comparing this with the total number $\binom{2n}{\log n}$ of I's yields

$$\frac{2\cdot\binom{7n/4}{\log n}}{\binom{2n}{\log n}} = 2\cdot \frac{7n/4 \dots (7n/4 - \log n+1)}{2n \dots\dots (2n - \log n+1)} \le 2\cdot (7/8)^{\log n} \to 0$$

for $n \to \infty$.

From now on we consider only I's with $I^c \cap \{1,\dots,n/4\} \neq \emptyset$ and $I^c \cap \{n+1,\dots,5n/4\} \neq \emptyset$. Consider any such I.

Then there is some x_i with $1 \leq i \leq n/4$ and some x_j with $n+1 \leq j \leq 5n/4$ such that $i,j \notin I$. A valuation of the variables in I does not fix the values of x_i and x_j, i.e. we are still free to choose the value of some low order bit in both factors of the multiplication. Consider two valuations val_1 and val_2 of the variables in I.

We extend val_1 and val_2 to valuations of all variables except x_i and x_j by assigning 0 to all variables in $I^c-\{x_i,x_j\}$. Under the extended valuation val_1 $\overline{Mult_n}$ computes the product $(B_1 + x_j \cdot 2^{j-(n+1)})(A_1 + x_i\ 2^{i-1})$ where A_1 is the integer represented by $val_1(x_n)\dots val_1(x_{i+1})0\ val_1(x_{i-1})\dots val(x_1)$ and similarly for val_2. Assume now that both valuations val_1 and val_2 produce the same function of the remaining variables.

Then in particular,

$$(B_1 + x_j\ 2^{j-(n+1)})\ (A_1 + x_1\ 2^{i-1}) =$$
$$(B_2 + x_j \cdot 2^{j-(n+1)})\ (A_2 + x_i\ 2^{i-1}) \bmod 2^n$$

and hence

$$A_1B_1 + A_1\ x_j\ 2^{j-(n+1)} + B_1\ x_i\ 2^{i-1} =$$
$$A_2B_2 + A_2\ x_j\ 2^{j-(n+1)} + B_2\ x_i\ 2^{i-1} \bmod 2^n.$$

Setting $x_i = 0$ and $x_j = 0$ yields

$$A_1B_1 = A_2B_2 \bmod 2^n$$

and hence

$$A_1x_j\ 2^{j-(n+1)} + B_1\ x_i\ 2^{i-1} =$$
$$A_2\ x_j\ 2^{j-(n+1)}+B_2\ x_i\ 2^{i-1} \bmod 2^n.$$

Setting now $x_i = 0$, $x_j = 1$ ($x_i = 1$, $x_j = 0$) yields

$$A_1 \, 2^{j-(n+1)} = A_2 \cdot 2^{j-(n+1)} \mod 2^n$$

and

$$B_1 \cdot 2^{i-1} = B_2 \, 2^{i-1} \mod 2^n$$

and hence

$$A_1 = A_2 \mod 2^{3n/4 + 1}$$

and

$$B_1 = B_2 \mod 2^{3n/4 + 1} \text{ since } i - 1 < n/4$$

and $j - (n+1) < n/4$. This shows that the two valuations val_1 and val_2 agree in the values assigned to x_i for $1 \le i \le 3n/4$ or $n + 1 \le i \le 7n/4$ and $i \in I$. Hence at least $2^{3n/2 - \log n}$ valuations of the variables in I yield different functions of the remaining variables.

These considerations show that $\overline{Mult}_n \in P_{p,q}^{(2n,n)}$ (0.1) for sufficiently large n and prove the theorem.

Bibliography

L.H. Harper: An n log n lower bound on synchronous combinational complexity, Dept. of Mathem.,UCR, Riverside

L.H. Harper & Savage: An $O(n^2 \log n^2)$ lower bound on the complexity of matrix multiplication, Carnegie Mellon Conference on the Complexity of Computing, 1976