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 paths from 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 $CS(f)$ 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

$Mult_n : \{0,1\}^{2n} \to \{0,1\}^{2n}$. It takes two $n$ bit binary numbers as inputs — $x_{2n} \cdots x_{n+1}$ and $x_n \cdots x_1$ (least significant bit to the right) — and produces the binary representation of the product of these two numbers.

Theorem: $CS(Mult_n) \geq O(n \log n)$

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

Definition: The class of functions $P_{p,q}^{n,m}(\epsilon)$, $0 \leq \epsilon < 1$, is defined as $P_{p,q}^{n,m}(\epsilon) = \{f: \{0,1\}^n \to \{0,1\}^m \mid \text{for all but a fraction } \epsilon \text{ of the subsets } I \subseteq \{1, \ldots, n\}, |I| = p, \text{ the set of } \text{n-p variables obtained by fixing the variables in } I \text{ in all possible } 2^p \text{ ways contains at least } q \text{ different functions} \}$. 
Fact (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 \( 0 \leq L \leq \max \{ 1; 2^{L-1} < p \text{ and } (1 - \varepsilon) \cdot \left[ 1 - \frac{2(n-p)2^{1}}{p-2^{1}} \right] \log q \geq m \} \)

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 \( \text{Mult}_n \) the following boolean function

\( \text{Mult}_n : \{0,1\}^{2n} + \{0,1\}^n \) defined as: \( \text{Mult}_n(x_{2n}...x_{n+1} x_n...x_1) \)

are the \( n \) least significant bits of the binary representation of the product of the two binary numbers represented by \( x_{2n}...x_{n+1} \) and \( x_n...x_1 \). Certainly

\[
C^S(\text{Mult}_n) \geq C^S(\text{Mult}_n)
\]

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

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

\[
\max \{ 1; \ 0.9. \left[ 1 - \frac{2 \log n \ 2^{1}}{2n - \log n - 2^{1}} \right] \log q \geq n \} \geq \max \{ 1; \ \frac{45}{40} \left[ 1 - \frac{2 \log n \ 2^{1}}{2n - \log n - 2^{1}} \right] n \geq n \}
\]

since \( \frac{3n}{2} - \log n \geq 5/4 \) for \( n \) sufficiently large

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

\[
= \max \{ 1; \ (18 \log n + 1) \cdot 2^{1} \leq 2n - \log n \} \]
\[\begin{align*}
\text{max} \{1; 1 &\leq \log (2n - \log n) - \log (18 \log n + 1)\} \\
&\geq 1/2 \log n \text{ for } n \text{ sufficiently large} \\
\text{and hence} \\
C^S(\text{Mult}_n) &\geq 0.9 \cdot (1/2 \log n - 4 \log n(\sqrt{n}-1) \over 2n-\log n - \sqrt{n})(3n/2-\log n) \\
&\geq 0.9 \cdot 1/4 \log n \cdot n \\
&\geq 1/5 \cdot n \cdot \log n
\end{align*}\]

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

Lemma 1: The fraction of the subsets \(I \subseteq \{1, \ldots, 2n\}\),

\(|I| = p \text{ with } \{1, \ldots, n/4\} \subset I \text{ or } \{n+1, \ldots, 5n/4\} \subset I\)
is less than 0.1 for sufficiently large \(n\).

Proof: \(I^C\), the complement of \(I\), is a subset of \(\{1, \ldots, 2n\}\) of size \(\log n\). The condition above is equivalent to \(I^C \cap \{1, \ldots, n/4\} = \emptyset\) or \(I^C \cap \{n+1, \ldots, 5n/4\} = \emptyset\). The number of \(I\)'s with

\(I^C \cap \{1, \ldots, n/4\} = \emptyset\) is equal to \(\binom{7n/4}{\log n}\) and hence the number of \(I\)'s with \(I^C \cap \{1, \ldots, n/4\} = \emptyset\) or \(I^C \cap \{n+1, \ldots, 5n/4\} = \emptyset\)
is less than \(2 \cdot \binom{7n/4}{\log n}\). Comparing this with the total number

\(\binom{2n}{\log n}\) of \(I\)'s yields

\[\frac{2 \cdot \binom{7n/4}{\log n}}{\binom{2n}{\log n}} = 2 \cdot \frac{7n/4 \ldots (7n/4 - \log n + 1)}{2n \ldots (2n - \log n + 1)} \leq 2 \cdot \frac{7/8}{\log n} \to 0\]

for \(n \to \infty\).
From now on we consider only $I$'s with $I^c \cap \{1, \ldots, n/4\} \neq \emptyset$ and $I^c \cap \{n+1, \ldots, 5n/4\} \neq \emptyset$. 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 $\text{val}_1$ and $\text{val}_2$ of the variables in $I$.

We extend $\text{val}_1$ and $\text{val}_2$ 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 $\text{val}_1$, $\text{Mult}_n$ computes the product

$$(B_1 + x_j \cdot 2^{j-(n+1)}) (A_1 + x_i \cdot 2^{i-1})$$

where $A_1$ is the integer represented by $\text{val}_1(x_n) \ldots \text{val}_1(x_{i+1}) 0 \text{ val}_1(x_{i-1}) \ldots \text{val}(x_1)$ and similarly for $\text{val}_2$. Assume now that both valuations $\text{val}_1$ and $\text{val}_2$ produce the same function of the remaining variables.

Then in particular,

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

$$(B_2 + x_j \cdot 2^{j-(n+1)}) (A_2 + x_i \cdot 2^{i-1}) \mod 2^n$$

and hence

$$A_1B_1 + A_1 x_j \cdot 2^{j-(n+1)} + B_1 x_i \cdot 2^{i-1} =$$

$$A_2B_2 + A_2 x_j \cdot 2^{j-(n+1)} + B_2 x_i \cdot 2^{i-1} \mod 2^n.$$
Setting now \( x_1 = 0, \ x_j = 1 \) \((x_1 = 1, \ x_j = 0)\)
yields
\[ A_1 \cdot 2^{j-(n+1)} = A_2 \cdot 2^{j-(n+1)} \mod 2^n \]
and
\[ B_1 \cdot 2^{i-1} = B_2 \cdot 2^{i-1} \mod 2^n \]
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 \( \text{val}_1 \) and \( \text{val}_2 \) agree in the values assigned to \( x_i \) for \( 1 \leq i \leq 3n/4 \) or \( n + 1 \leq i \leq 7n/4 \) 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 \( \text{Mult}_n \in p^{(2n,n)}_{p,q} \) \((0.1)\) 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