A long note on Mulders' short product

G. Hanrot and P. Zimmermann (LORIA-INRIA Lorraine)

March 28, 2006

Abstract

The short product of two power series is the meaningful part of the product of these objects, *i.e.*, $\sum_{i+j<n} a_i b_j x^{i+j}$. In [2], Mulders gives an algorithm to compute a short product faster than the full product in the case of Karatsuba's multiplication [1]. This algorithm work by selecting a cutoff point k and performing a full $k \times k$ product and two $(n-k) \times (n-k)$ short products recursively. Mulders also gives an heuristically optimal cutoff point βn. In this paper, we determine the optimal cutoff point in Mulders' algorithm. We also give a slightly more general description of Mulders' method.

Cyrano

Ah ! non ! c'est un peu court, jeune homme !
On pouvait dire... Oh ! Dieu !... Bien des choses en somme...

E. Rostand, *Cyrano de Bergerac*

1 Introduction

Let $A = \sum_{0 \le i < n} a_i x^i + O(x^n)$ and $B = \sum_{0 \le i < n} b_i x^i + O(x^n)$ be two power series. Their product is naturally defined as $\sum_{0 \le i < n} (\sum_{j+k=i} a_j b_k) x^i + O(x^n)$. We shall call this operation the *short product* of A and B, and note it $AB \bmod x^n$.

A trivial way to compute a short product is to compute the full product and discard the high order terms. It has long been an open problem to know whether it is possible to compute a short product faster than a full one in a subquadratic multiplication model. In [2], Mulders gives a positive answer, on average, under a multiplication model $\approx n^\alpha$ with $1 < \alpha < 2$.

Mulders' algorithm consists in writing $A_i = P_i + x^k Q_i$, $i = 1, 2$ where $\deg(P_i) < k$, with $k \ge n/2$. Then, $A_1 A_2 \equiv P_1 P_2 + x^k (Q_1 P_2 + P_1 Q_2 \bmod x^{n-k}) \bmod x^n$. Namely, a short product of two order n power series can be computed as a full product of two order k power series, and two short products of order $n-k$ power series, plus some operations of lower complexity.

The main question with Mulders' algorithm is to find the optimal cutoff point k, which achieves the number of multiplications given by

$$S(n) = \min_{n/2 \le k \le n} \left(M(k) + 2S(n-k) \right),$$

where $M(n)$ (resp. $S(n)$) denotes the complexity of a full product (resp. short product) of order n power series.

In his paper, Mulders gives an heuristic analysis based on the approximation $M(n) \approx n^\alpha$ and searches for a value of k of the form βn. A heuristic optimal cutoff point is then obtained for the Karatsuba model ($\alpha = \log_2 3$), with $\beta \approx 0.694$.

In the present paper we prove that the optimal cutoff point is obtained for $k = 2^{\lfloor \log_2 n \rfloor}$ in the Karatsuba model (§2). In §3, we present a variant of Mulders' algorithm, which directly achieves the optimal cutoff under the Karatsuba model. Finally, in §4, we generalize the analysis to a non-trivial break-even point between quadratic and sub-quadratic multiplication.

2 The optimal cutoff point

Let $M(n)$ be the number of multiplications of a full product, and

$$S(n) = \min_{n/2 \le k \le n} \left(M(k) + 2S(n-k) \right)$$

the number of multiplications of Mulders' short product.

Lemma 1 *We have $S(n+1) \ge S(n)$ for all n, as long as $M(n)$ is non decreasing.*

Proof. Let $s(n)$ be an optimal cutoff point for n (there may be several). If $s(n+1) = n+1$, we have $S(n+1) = M(n+1) \ge M(n) \ge S(n)$. Otherwise we have

$$\begin{aligned}
S(n) &\le M(s(n+1)) + 2S(n - s(n+1)) \\
&\le M(s(n+1)) + 2S(n+1-s(n+1)) - 2[S(n+1-s(n+1)) - S(n-s(n+1))] \\
&\le S(n+1) - 2[S(n+1-s(n+1)) - S(n-s(n+1))],
\end{aligned}$$

from which the lemma follows by induction.

We assume from now on the Karatsuba model $M(n) = K(n)$ for full products, given by $K(1) = 1$, and $K(n) = 2K(\lceil \frac{n}{2} \rceil) + K(\lfloor \frac{n}{2} \rfloor)$ for $n \ge 2$.

Lemma 2 *Let $S(n)$ be the number of operations in Mulders' algorithm with optimal cutoff point. Then we have $S(1) = 1$, $S(n) \ge S(\lceil n/2 \rceil) + 2S(\lfloor n/2 \rfloor)$.*

Proof.

By induction, the cases $n = 1$ and $n = 2$ being trivial.

Assume that the relation above is true for $k < n$. We have, by definition and induction,

$$
\begin{aligned}
S(n) &= \min_{\lceil \frac{n}{2} \rceil \le \ell \le n} (K(\ell) + 2S(n-\ell)) \\
&\ge \min_{\lceil \frac{n}{2} \rceil \le \ell \le n} \left(2K\left(\left\lceil \frac{\ell}{2} \right\rceil\right) + K\left(\left\lfloor \frac{\ell}{2} \right\rfloor\right) + 2S\left(\left\lceil \frac{n-\ell}{2} \right\rceil\right) + 4S\left(\left\lfloor \frac{n-\ell}{2} \right\rfloor\right)\right), \\
&\ge 2 \min_{\lceil \frac{n}{2} \rceil \le \ell \le n} \left(K\left(\left\lceil \frac{\ell}{2} \right\rceil\right) + 2S\left(\left\lfloor \frac{n-\ell}{2} \right\rfloor\right)\right) \\
&\quad + \min_{\lceil \frac{n}{2} \rceil \le \ell \le n} \left(K\left(\left\lfloor \frac{\ell}{2} \right\rfloor\right) + 2S\left(\left\lceil \frac{n-\ell}{2} \right\rceil\right)\right).
\end{aligned}
$$

Assume first that $n = 2n_1 + 1$ and $\ell = 2\ell_1 + 1$ are odd. Then

$$
\begin{aligned}
S(n) \ge 2 \min_{\lceil \frac{n_1+1}{2} \rceil \le \ell_1 + 1 \le n_1 + 1} (K(\ell_1 + 1) &+ 2S((n_1+1) - (\ell_1+1))) \\
&+ \min_{\lceil \frac{n_1}{2} \rceil \le \ell_1 \le n_1} (K(\ell_1) + 2S(n_1 - \ell_1)),
\end{aligned}
$$

and the right hand side is just $2S(n_1+1) + S(n_1) \ge S(\lceil \frac{n}{2} \rceil) + 2S(\lfloor \frac{n}{2} \rfloor)$, according to Lemma 1.

Assume that n or ℓ is even. Then we have $\lceil \frac{n-\ell}{2} \rceil = \lceil \frac{n}{2} \rceil - \lfloor \frac{\ell}{2} \rfloor$ and $\lfloor \frac{n-\ell}{2} \rfloor = \lfloor \frac{n}{2} \rfloor - \lceil \frac{\ell}{2} \rceil$; furthermore $\lceil \frac{\ell}{2} \rceil \le \lfloor \frac{n}{2} \rfloor$ since $\ell \le n$. Hence,

$$
\begin{aligned}
S(n) \ge 2 \min_{\left\lceil \frac{\lceil \frac{n}{2} \rceil}{2} \right\rceil \le \lceil \frac{\ell}{2} \rceil \le \lfloor \frac{n}{2} \rfloor} &\left(K\left(\left\lceil \frac{\ell}{2} \right\rceil\right) + 2S\left(\left\lfloor \frac{n}{2} \right\rfloor - \left\lceil \frac{\ell}{2} \right\rceil\right)\right) \\
+ \min_{\left\lfloor \frac{\lceil \frac{n}{2} \rceil}{2} \right\rfloor \le \lfloor \frac{\ell}{2} \rfloor \le \lfloor \frac{n}{2} \rfloor} &\left(K\left(\left\lfloor \frac{\ell}{2} \right\rfloor\right) + 2S\left(\left\lceil \frac{n}{2} \right\rceil - \left\lfloor \frac{\ell}{2} \right\rfloor\right)\right).
\end{aligned}
$$

The first term is always larger than $2S(\lfloor \frac{n}{2} \rfloor)$, whereas the second one might be smaller than $S(\lceil \frac{n}{2} \rceil)$ only when $n = 4k+1$ or $n = 4k+2$, for the choice $\lfloor \frac{\ell}{2} \rfloor = k$. However, if $n = 4k+1$, the only even value for ℓ is $2k$, which violates the condition $\ell \ge \lceil \frac{n}{2} \rceil$; and if $n = 4k+2$, the only choice satisfying $\ell \ge \lceil \frac{n}{2} \rceil$ is $\ell = n/2$, which gives $S(n) = K(n/2) + 2S(n/2) \ge 3S(n/2)$. Hence we can assume that the second term is larger than $S(\lceil \frac{n}{2} \rceil)$, from which the result follows.

Lemma 3 *Let $S^*(n)$ be the number of multiplications obtained with cutoff point $s(n) = 2^{\lfloor \log_2 n \rfloor}$. Then $S^*(1) = 1$, $S^*(n) = S^*(\lceil \frac{n}{2} \rceil) + 2S^*(\lfloor \frac{n}{2} \rfloor)$.*

PROOF. By induction. This is obvious for $n = 1$. Assume the result is true for $n \in [2^k, 2^{k+1}[$. Then we have $S^*(2n) = K(2^{k+1}) + 2S^*(2(n-2^k)) = 3(K(2^k) + 2S^*(n-2^k)) = 3S^*(n)$ by induction, and $S^*(2n+1) = K(2^{k+1}) + 2S^*(2(n-2^k)+1) = 3K(2^k) + 2S^*(n+1-2^k) + 4S^*(n-2^k)$. If $n+1 < 2^{k+1}$, we get $3K(2^k) + 2S^*(n+1-2^k) + 4S^*(n-2^k) = S^*(n+1) + 2S^*(n)$. (In the special case $n+1 = 2^{k+1}$, the identity holds too since $K(2^k) = S^*(2^k) = 3^k$.) REMARK: for $n = 2^k$, both cutoffs $s = 2^k$ and $s = 2^{k-1}$ give the same value, thus Lemma 3 remains true if we replace $2^{\lfloor \log_2 n \rfloor}$ by $2^{\lfloor \log_2 (n-1) \rfloor}$.

Theorem 1 *For Karatsuba multiplication, an optimal cutoff point in Mulders' algorithm is obtained for* $k = 2^{\lfloor \log_2 n \rfloor}$, *and* $S(n) = S(\lceil \frac{n}{2} \rceil) + 2S(\lfloor \frac{n}{2} \rfloor)$.

PROOF. By definition, we have $S^*(n) \geq S(n)$. By an easy induction, using Lemmas 2 and 3, we have $S^*(n) \leq S(n)$. The theorem follows.

It is easily seen that $\limsup S(n)/K(n) = 1$, e.g. for $n = 2^t$. If one takes $x_n = \frac{1}{3}(4^{n+1} - 1)$, easy calculations lead to $\lim S(x_n)/K(x_n) = \frac{3}{5}$, and from an experimental viewpoint it seems to be the value of $\liminf S(n)/K(n)$. The average of $S(n)/K(n)$ for $n \leq 2^{26}$ is 0.705754. Note that these values are better than expected from Mulders' heuristic analysis.

3 A variant of Mulders' algorithm

We can see Karatsuba's algorithm the following way: the module $K_n[x]$ of truncated Taylor series of order n (*i.e.*, degree less than n) can be written as $K_{\lfloor n/2 \rfloor}[x] \oplus x^{\lfloor n/2 \rfloor} K_{\lceil n/2 \rceil}[x]$. Then to any $P \in K_n[x]$ we can associate $Q \in K[x,t] = Q_1 + Q_2 t$; following the well-known interpretation of Karatsuba's algorithm as an evaluation-interpolation algorithm we can see Q_1 as the value at 0 and Q_2 as the value at ∞. Knowing the value at a third point (usually 1, *i.e.*, $Q_1 + Q_2$) allows then one to reconstruct the product.

We can use a slightly different decomposition in that case: put $K_n[x] = O_{\lceil n/2 \rceil}[x] \oplus x O_{\lfloor n/2 \rfloor}[x]$, where $O_k[x] = \{P(x^2), P \in K_k[x]\}$. Then, as in the preceding case, to P we can associate $Q = Q_1 + Q_2 t$. Assume that Q and Q' are series of order n. Then, to compute the short product QQ', we need the lower n terms of $QQ' = Q_1 Q'_1 + t(Q_1 Q'_2 + Q_2 Q'_1) + t^2 Q_2 Q'_2$.

This means that we need

- the lower n terms of $Q_1 Q'_1$, which can be obtained by a short product of Q_1 by Q'_1 of size $\lceil \frac{n}{2} \rceil$ (recall that Q_1 and Q'_1 are even series of order n);
- the lower $n-1$ terms of $(Q_1 + Q_2)(Q'_1 + Q'_2) - Q_1 Q'_1 - Q_2 Q'_2$; if the lower $n-1$ terms of $Q_1 Q'_1$ and $Q_2 Q'_2$ are known, this amounts to a short product of $(Q_1 + Q_2)$ by $(Q'_1 + Q'_2)$ of order $\lceil \frac{n-1}{2} \rceil$;
- the lower $n-2$ terms of $Q_2 Q'_2$; however for the above middle term we need the lower $n-1$ terms, which can be obtained by a short product of Q_2 by Q'_2 of order $\lceil \frac{n-1}{2} \rceil$.

From these remarks we can extract the following algorithm:

Algorithm ShortProduct
Input: $f, g \in R[x]$, n a positive integer.
Output: $fg \bmod x^n$.
if $n = 1$ **then**
  return$(fg \bmod x)$
fi;
$n_0 := \lfloor n/2 \rfloor, n_1 := \lceil n/2 \rceil$
decompose f into $f_{\text{even}}(x^2) + x f_{\text{odd}}(x^2)$
$l :=$ ShortProduct$(f_{\text{even}}, g_{\text{even}}, n_1)$
$h :=$ ShortProduct$(f_{\text{odd}}, g_{\text{odd}}, n_0)$
$m :=$ ShortProduct$(f_{\text{even}} + f_{\text{odd}}, g_{\text{even}} + g_{\text{odd}}, n_0) - l - h$
return$(l(x^2) + xm(x^2) + x^2 h(x^2))$

Theorem 2 *Algorithm ShortProduct is correct, and performs the same number of ring multiplications than Mulders' algorithm for the Karatsuba model, with the optimal cutoff value* $s = 2^{\lfloor \log_2 n \rfloor}$.

Proof. We prove both the correctness and the optimality by induction on n. For $n = 1$, the statement of the Theorem holds. Now let us assume it holds up to $n - 1$ for $n \geq 2$. As $n_0, n_1 < n$, we have by induction $l(x^2) = f_{\text{even}}(x^2) g_{\text{even}}(x^2) \bmod x^{2n_1}$, $x^2 h(x^2) = f_{\text{odd}}(x^2) g_{\text{odd}}(x^2) \bmod x^{2n_0+2}$, and $xm(x^2) = x(f_{\text{even}}(x^2) g_{\text{odd}}(x^2) + f_{\text{odd}}(x^2) g_{\text{even}}(x^2)) \bmod x^{2n_0+1}$, which implies $l(x^2) + xm(x^2) + x^2 h(x^2) = fg \bmod x^n$ since $\min(2n_1, 2n_0 + 1) = n$.

Remark. — Practical comparisons of Mulders' method and ours are given in §5 in the case of short products of polynomials in $F_p[X]$.

4 Mulders' algorithm with quadratic multiplication for small sizes

Even though Karatsuba's algorithm has a better asymptotic complexity than naive multiplication, in practice for small sizes the latter performs much better except maybe when multiplication in the base ring is very costly so that it is crucial to make as few of them as possible. As a consequence, many multiprecision multiplication code use the naive, quadratic algorithm for small values, and switches to Karatsuba's method for larger values.

Hence Mulders' practical optimal cutoff point should be very different from what was found in the first section of this paper.

There are two approaches to this, if one assumes that naive multiplication is used for $n \leq n_0$.

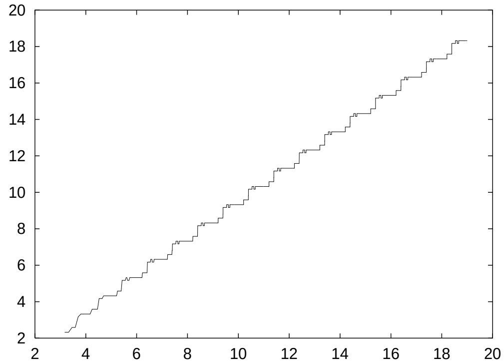
- Multiplication is performed blockwise, *i.e.*, the numbers are first cut into pieces of size n_0, and multiplication at the block level are done by quadratic algorithms.

- Multiplication is performed wordwise, *i.e.*, Karatsuba's method is used for numbers larger than n_0 words, and a quadratic method below.

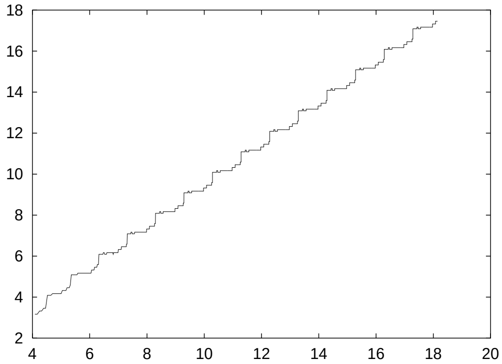
In the first case, the number of multiplications for two numbers of n blocks only changes the value of $S(1) = 1/2$ whereas $K(1) = 1$. One can prove that the optimal strategy is then exactly the same that in the previous situation, except that if $n = 2^k$ one should take $n = 2^{k-1}$ as a splitting point (*cf.* the remark following Lemma 3).

In the second case, things are more complicated. A first way to deal with the problem is to modify the initialization by using $K(n) = n^2$, $S(n) = n(n+1)/2$ for $n \leq n_0$. We have not been able in that case to find the optimal splitting point in full generality, but we can report on experiments.

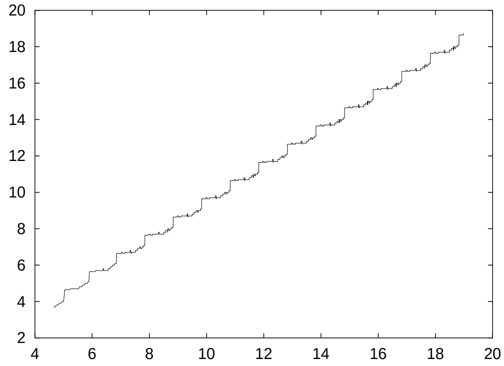
We give below diagrams of the optimal cutoff points when $n_0 = 8$, $n_0 = 16$, $n_0 = 24$ and $n_0 = 32$ in logarithmic scales for both coordinates, for n up to 2^{17}.



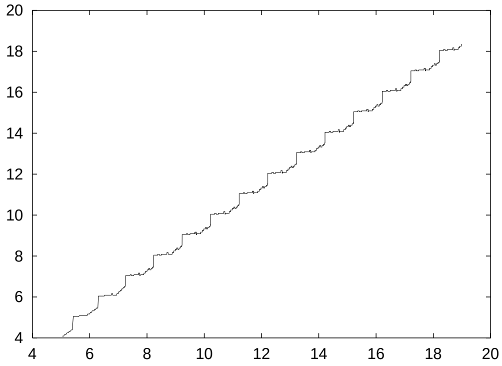
$n_0 = 8$



$n_0 = 16$



$n_0 = 24$



$n_0 = 32$

The main remark that can be done is that these diagrams are almost autosimilar, *i.e.*, that the splitting point for $2n$ seems to be twice the splitting point for n.

A natural strategy is derived from this remark: choose some multiple n_1 of n_0 and tabulate the optimal cutoff $s(k)$ value for $n_1/2 < n \leq n_1$. For a given N, we search for t such that $n_1/2 < N/2^t \leq n_1$, and choose as a cutoff the value $2^t s(N/2^t)$. The results obtained with this strategy are given in Table 1, where the columns show up to what value

	S_{2n_0}	S_{4n_0}	S_{6n_0}	S_{8n_0}	Mulders' strategy
$n_0 = 8$	28%	11%	4%	4%	13%
$n_0 = 16$	29%	6%	4%	4%	20%
$n_0 = 24$	29%	8%	4%	4%	23%
$n_0 = 32$	29%	9%	4%	3%	24%

Table 1: Loss with respect to the optimal choice.

the optimal cutoff has been tabulated, and we show the maximal difference between the optimal strategy and the present strategy, and between Mulders' strategy and the optimal strategy. Let $S_{n_1}(n)$ be the value obtained by this strategy; Table 1 shows the loss in terms of number of multiplications, with respect to the optimal choice.

In this context, the variant of Section 3 has much more interest, as shows the following.

Theorem 3 *Assume that a quadratic algorithm is used for $n \le n_0$, so let $\tilde{S}(n)$ be the number of ring multiplications performed by the variant of section 3 and $S_{\text{opt}}(n)$ the number of multiplications performed by Mulders' algorithm with optimal cutoff. Then $\tilde{S}(n) < S_{\text{opt}}(n)$ for all $n > n_0$ as soon as $n_0 \ge 4$.*

To prove that theorem, we first prove two lemmas.

Lemma 4 $S_{\text{opt}}(n) > \tilde{S}(n)$ *for* $n_0 < n \le 2n_0$.

Proof. For $2 \le n \le n_0$, $K(n) = n^2$, and $S_{\text{opt}}(n) = \tilde{S}(n) = n(n+1)/2$. Assume now $n_0 < n \le 2n_0$: $K(n) = 2\left\lceil \frac{n}{2} \right\rceil^2 + \left\lfloor \frac{n}{2} \right\rfloor \ge \frac{3}{4}n^2$; $\tilde{S}(n) = \frac{3}{2}k^2 + \frac{3}{2}k$ for $n = 2k$, and $\tilde{S}(n) = \frac{3}{2}k^2 + \frac{5}{2}k + 1$ for $n = 2k+1$. $S_{\text{opt}}(n) = \min_{n/2 \le l \le n} K(l) + 2S_{\text{opt}}(n-l) \ge \min_{n/2 \le l \le n} \frac{3}{4}l^2 + (n-l)(n-l+1) \ge \frac{12}{7}k^2 + \frac{6}{7}k - \frac{1}{7}$ for $n = 2k$, and $\ge \frac{12}{7}k^2 + \frac{18}{7}k + \frac{5}{7}$ for $n = 2k+1$. It follows that $S_{\text{opt}}(n) > \tilde{S}(n)$ for $k \ge 4$ in case $n = 2k$ (*i.e.* $n \ge 8$), and $k \ge 2$ in case $n = 2k+1$ (*i.e.* $n \ge 5$). The only uncovered cases are $n = 6$ for $n_0 = 4$ or 5, in which case we have $S_{\text{opt}}(n) = 21$ and $\tilde{S}(n) = 18$.

Lemma 5 $S_{\text{opt}}(n) \ge S_{\text{opt}}(\left\lceil \frac{n}{2} \right\rceil) + 2S_{\text{opt}}(\left\lfloor \frac{n}{2} \right\rfloor)$.

Proof. We first prove by induction that $S_{\text{opt}}(n-1) \le S_{\text{opt}}(n) < K(n)$ for $n \ge 2$: For $n \le n_0$, $K(n) - S_{\text{opt}}(n) = n(n-1)/2 > 0$, and $S_{\text{opt}}(n) = n(n+1)/2 \ge n(n-1)/2 = S_{\text{opt}}(n-1)$.

For $n > n_0$, $K(n) = 2K(\left\lceil \frac{n}{2} \right\rceil) + K(\left\lfloor \frac{n}{2} \right\rfloor) > K(\left\lceil \frac{n}{2} \right\rceil) + S_{\text{opt}}(\left\lceil \frac{n}{2} \right\rceil) + S_{\text{opt}}(\left\lfloor \frac{n}{2} \right\rfloor) \ge K(\left\lceil \frac{n}{2} \right\rceil) + 2S_{\text{opt}}(\left\lfloor \frac{n}{2} \right\rfloor) \ge S_{\text{opt}}(n)$. To prove $S_{\text{opt}}(n-1) \le S_{\text{opt}}(n)$, we distinguish the case $n = n_0 + 1$. In that case $S_{\text{opt}}(n-1) = n_0(n_0+1)/2$, and $S_{\text{opt}}(n) = \min_{\frac{n}{2} \le l \le n} l^2 + (n-l)(n-l+1)$. The minimum for integer l is attained at $l = \left\lceil \frac{n}{2} \right\rceil$, with value $n(n+1)/2$. Thus for $n = n_0 + 1$, $S_{\text{opt}}(n) = n(n+1)/2 \ge n(n-1)/2 = S_{\text{opt}}(n-1)$. For $n > n_0 + 1$, the case $s(n) = n$ cannot happen because $S_{\text{opt}}(n) < K(n)$, and the second part of the proof of Lemma 1 applies, thus $S_{\text{opt}}(n-1) \le S_{\text{opt}}(n)$.

Then Lemma 2 still holds for $S := S_{\text{opt}}$, since its proof just uses the fact that S is non-decreasing, the inequality $K(n) \geq 2K(\lceil \frac{n}{2} \rceil) + K(\lfloor \frac{n}{2} \rfloor)$ — which holds for $n \geq 2$ whatever the value of $n_0 \geq 2$ — and the fact that $K(n) \geq S_{\text{opt}}(n)$. PROOF.[Proof of Theorem 3] Let $T(n) = S_{\text{opt}}(n) - \tilde{S}(n)$. We have $T(n) = 0$ for $n \leq n_0$, $T(n) > 0$ for $n_0 < n \leq 2n_0$ (Lemma 4) and $T(n) \geq T(\lceil \frac{n}{2} \rceil) + 2T(\lfloor \frac{n}{2} \rfloor)$ for $n > 2n_0$ (Lemma 5 together with $\tilde{S}(n) = \tilde{S}(\lceil \frac{n}{2} \rceil) + 2\tilde{S}(\lfloor \frac{n}{2} \rfloor)$). In the latter case, since $\lceil \frac{n}{2} \rceil > n_0$, it follows by induction that $T(n) > 0$ for $n > n_0$.

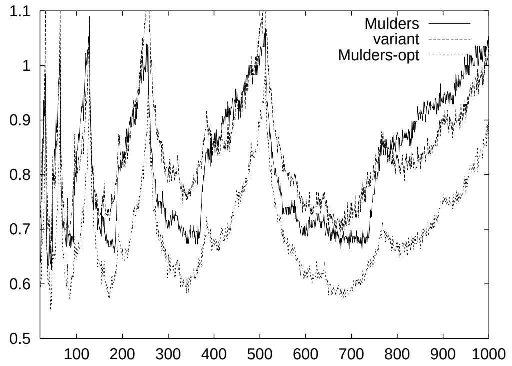
In terms of number of multiplications, $\tilde{S}(n)$ is between 10% and 40% smaller than $S_{\text{opt}}(n)$.

5 Implementation results

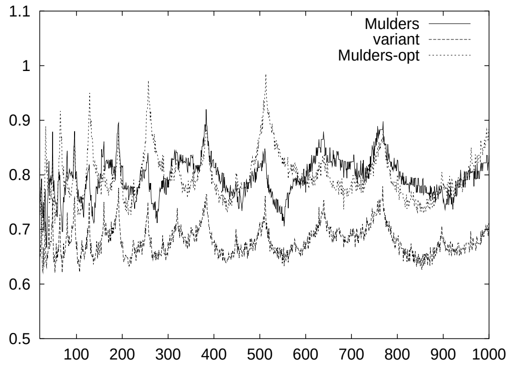
We report shortly on implementation results in this section. We have implemented the case of polynomials over a finite field F_p, chosen so that p^2 fits into a single machine word. We compare the results for 3 algorithms, namely Mulders' with cutoff at $\lfloor \beta n \rfloor$, Mulders' with theoretical optimal cutoff (we took here $2^{\lfloor \log(n-1) \rfloor}$), our variant.

The results displayed below have been obtained on an Alpha ev6 500 MHz. We give figures for a break-even point at $n_0 = 4, 8, 16$, and for the situation where only Karatsuba is used ($n_0 = 1$).

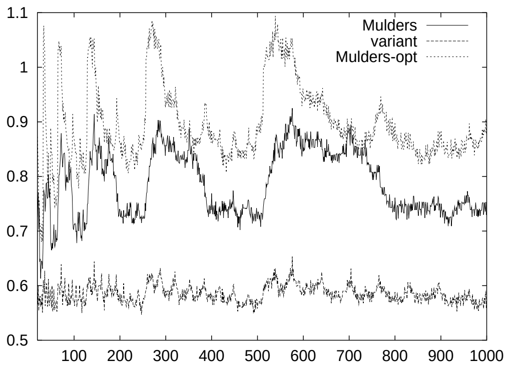
Note that the figure displays the quotient of the time for a short product by the time for a full product of the same size.

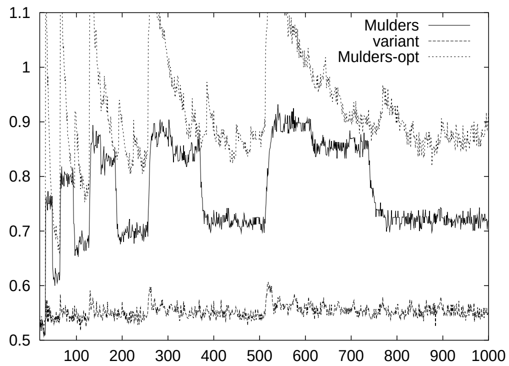


Various short product algorithms, $n_0 = 1$



Various short product algorithms, $n_0 = 8$





Various short product algorithms, $n_0 = 16$ Various short product algorithms, $n_0 = 32$

We remark the following:

- For $n_0 > 1$, our variant beats almost always the two others algorithms; when n_0 grows this is more and more true.
- Mulders with optimal cutoff is very disappointing (though sometimes better than Mulders' cutoff), except for $n_0 = 1$. The quadratic behaviour for small values seems to make the study of Section 2 incorrect.

Note however that floating-point experiments would probably come down to very different conclusions, since the carries are a simple matter to deal with in Mulders' method but are a real problem with our variant.

6 Generalizations

A natural question is to know whether the variant shown above extends to the case where the polynomial is split into more than two parts (Toom-Cook's algorithm). We give a few hints on how the previous results generalize in this setting.

A difficult problem is already to obtain the recurrence relation giving $TC_r(n)$ in Toom-Cook's case, as simple modifications give rather different recurrences and thus different functions $TC_r(n)$. We shall limit ourselves to the case $r = 3$ (usually, Toom-Cook with $r = 4$ is superseded by FFT techniques). The best recurrence that we obtained for Toom-Cook is then $TC(1) = 1$, $TC(2) = 3$, $TC(n) = 3TC(\lfloor (n+2)/3 \rfloor) + TC(\lfloor (n+1)/3 \rfloor) + TC(\lfloor n/3 \rfloor)$.

With this recurrence relation, it can be proved (and this seems to remain true for higher values of r for the obvious similar choice of splitting point, though we did not try to prove it) that the optimal splitting point in Mulders' algorithm for an operand of size n is the largest number of the form $x3^y$ with $x < 3$ which is smaller or equal than n. This gives the recurrence relations $SP(n) = SP(\lfloor (n+2)/3 \rfloor) + 2SP(\lfloor (n+1)/3 \rfloor) + 2SP(\lfloor n/3 \rfloor)$.

Our variant now amounts to split the polynomial in 3 parts, according to the classes of the degrees modulo 3; it still works. However, in that case it gives results which are worse than Mulders' method with optimal cutoff; the corresponding recurrence relation is indeed $\tilde{S}(n) = \tilde{S}(\lfloor (n+2)/3 \rfloor) + 3\tilde{S}(\lfloor (n+1)/3 \rfloor) + \tilde{S}(\lfloor n/3 \rfloor)$.

Note however that all these comparisons in terms of number of multiplications should be validated by practical implementations.

7 Conclusion

We have given an exact analysis of Mulders' short product in Karatsuba's case. This allows to find the optimal splitting point. The gain over a full product with this cutoff is on average of 30% in Karatsuba's case, in terms of the number of multiplications. In practice, we give an heuristic allowing one to obtain a cutoff point not to far from optimal; the gain over Mulders' heuristic is roughly 15%.

8 Acknowledgements

The authors wish to thank Michel Quercia for valuable discussions and a useful collaboration on related subjects.

References

[1] Karatsuba, A. A., and Ofman, Y. P. Multiplication of multiplace numbers by automata. Dokl. Akad. Nauk SSSR **145**, 2, 293–294 (1962).

[2] Mulders, T. On short multiplications and division. AAECC **11**, 1, 69–88 (2000).