Towards Optimal Toom-Cook Matrices

for Integer and Polynomial Multiplication

Marco Bodrato, Alberto Zanoni

Centro "Vito Volterra"
Università di Roma "Tor Vergata"
Via Columbia 2 – 00133 Rome, Italy

{bodrato, zanoni}@volterra.uniroma2.it

ISSAC 2007

July 31st

1. Toom-Cook multiplication methods
   - Multiplication algorithms and complexity
   - Toom-Cook algorithm for polynomials, revisited
   - Extension to unbalanced factors
2. Toom matrices
   - The working model
   - Operations and costs
   - Graph searching
3. Results
   - Toom-2.5 and Toom-3
   - Higher Toom-Cook methods
   - Some graphics

Long integer and polynomial multiplication

Some notation

Let **R** be $\mathbb{Z}$ or $\mathbb{Z}[X]$,

$$a(x) = \sum_{i=0}^{d_a} a_i x^i \quad , \quad b(x) = \sum_{i=0}^{d_b} b_i x^i \in \mathbf{R}[x]$$

We want to compute their product

$$c(x) = \sum_{i=0}^{d_c} c_i x^i \in \mathbf{R}[x]$$

$$\deg(a) = d_a \quad ; \quad \deg(b) = d_b \quad ; \quad \deg(c) = d_c = d_a + d_b$$

Long integer and polynomial multiplication

The classical Toom-Cook approach

- Toom-Cook methods concern univariate polynomials multiplication.
- Toom-n method refers to factors having n parts each (degrees $d_a = d_b = n - 1$).
- It is an absolutely standard procedure to apply these methods to general univariate polynomials and long integers multiplication by a simple base changing.

Multiplication algorithms

Many algorithms are known for polynomial multiplication.

- Naïve $O(d^2)$

Each one has a different complexity, and its own range where it is the fastest one.

Multiplication algorithms

Many algorithms are known for polynomial multiplication.

- Naïve $\mathrm{O}(d^2)$
- Karatsuba (1962) $\mathrm{O}(d^{\log_2 3})$

Each one has a different complexity, and its own range where it is the fastest one.

Multiplication algorithms

Many algorithms are known for polynomial multiplication.

- Naïve $O(d^2)$
- Karatsuba (1962) $O(d^{\log_2 3})$
- Schönhage-Strassen (1971) $O(d \log d \log \log d)$

Each one has a different complexity, and its own range where it is the fastest one.

In 2007, Martin Fürer announced a new algorithm that should have a better asymptotic complexity.

Multiplication algorithms

Many algorithms are known for polynomial multiplication.

- Naïve $O(d^2)$
- Karatsuba (Toom-2) (1962) $O(d^{\log_2 3})$
- Toom-Cook-n (1963) $O(d^{\log_n(2n-1)})$
- Schönhage-Strassen (1971) $O(d \log d \log \log d)$

Each one has a different complexity, and its own range where it is the fastest one.

We aim to analyse the optimality of Toom-Cook methods within their respective ranges of applicability.

Recall on Toom-n algorithm

3 (core) phases

1. Splitting: choose a base and split
2. Evaluation

5. Recomposition: shift and add.

Phase 2, some linear algebra

Evaluate polynomials $a(x), b(x)$ in $2n-1$ different points $\{v_i\} \in \mathbb{Z}$.

This can be obtained by multiplying a (non square) Vandermonde matrix by the vector of coefficients.

Recall on Toom-n algorithm

3 (core) phases

1. Splitting: choose a base and split
2. Evaluation: $2 \times$ matrix-vector multiplication
3. Multiplication

5. Recomposition: shift and add.

Phase 3, recursive application

see unbalanced

Evaluate the product by multiplying factors evaluations.

$c(v_i) = a(v_i) \cdot b(v_i)$

(degree $n-1$) $\times$ (degree $n-1$) $\rightsquigarrow$ degree $2n-2$.

(n parts) $\times$ (n parts) $\rightsquigarrow$ $2n-1$ parts. $\Rightarrow$ $2n-1$ multiplications.

Recall on Toom-n algorithm

3 (core) phases

1. Splitting: choose a base and split
2. Evaluation: $2 \times$ matrix-vector multiplication
3. Multiplication: $(2n-1) \times$ smaller multiplication
4. Interpolation
5. Recomposition: shift and add.

Phase 4, some more linear algebra

Interpolate to obtain coefficient of the product polynomial.

Obtain this by multiplying the inverse of a (square) Vandermonde matrix by the vector of evaluations.

Recall on Toom-n algorithm

3 (core) phases

1. Splitting: choose a base and split
2. Evaluation: $2 \times$ matrix-vector multiplication
3. Multiplication: $(2n-1) \times$ smaller multiplication
4. Interpolation: *inverse matrix*-vector multiplication
5. Recomposition: shift and add.

Phases 2 and 4 are critical

Splitting order n results in $(2n-1)$ multiplications in phase 3, and asymptotic behaviour $\Theta(d^{\log_n(2n-1)})$. Rigidly.
The hidden constant is determined by the evaluation/interpolation points and operation sequences for phases 2 and 4.

Unbalanced operands

Factors with different degrees

Toom-(n+m)/2

back to balanced

(degree $n-1$) $\times$ (degree $m-1$) $\rightsquigarrow$ degree $n+m-2$
(n parts) $\times$ (m parts) $\rightsquigarrow$ $n+m-1$ parts

Toom methods can thus be applied also to polynomials with different degrees. The evaluation phase depends on m and n separately, while the interpolation phase only on $n+m$.

Toom-2.5	Unbalanced Toom-3
(deg 2) $\times$ (deg 1) $\rightsquigarrow$ deg 3	(deg 3) $\times$ (deg 1) $\rightsquigarrow$ deg 4
(3 parts) $\times$ (2 parts) $\rightsquigarrow$ 4 parts	(4 parts) $\times$ (2 parts) $\rightsquigarrow$ 5 parts

Some examples for basic cases

The matrices of Toom-2.5 and Toom-3 interpolation phase are

$$A_{2.5} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad ; \quad A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 16 & 8 & 4 & 2 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem

For $n \geqslant 3$, $\det(A_n)$ is not a power of 2 (one division is needed).

Theorem

Let A_n be generated by $\{\infty, 1, -1, v_4, \dots, v_{2n-2}, 0\}$. At most $2n-5$ divisions are needed in the interpolation phase.

The setting

GOAL: we want the best (most efficient) sequence of elementary operations on rows to transform matrix A_n into identity.

- There are ∞ possible inversion sequences (IS).
- We restrict the admissible operations by defining two criteria.
- They define a finite "model" such that an exhaustive search is possible.
- We describe this model as a weighted graph.
- The goal is reached by solving a shortest path problem on the graph.

Some useful definitions

For a square matrix M:

$M[i,j]$	:	the entry in position (i,j)
$M^{(i)}$	:	the i^{th} line
$M^{[j]}$	:	the j^{th} column

Definition

The **support** of $M^{(i)}$ is the set $s(M^{(i)})$ of column indexes $j \in \mathbb{N}$ such that $M[i,j] \neq 0$. Similarly for $M^{[i]}$.
The **support** of M is the set $s(M)$ of pairs $(i,j) \in \mathbb{N} \times \mathbb{N}$ such that $M[i,j] \neq 0$.

${}^{\#}M^{(i)}$ = cardinality of $s(M^{(i)})$. Similarly for ${}^{\#}M^{[i]}$ and ${}^{\#}M$.

The model criteria

$$\cdots \to M \xrightarrow{(i)} \widetilde{M} \to \cdots \to I$$

(A) **Support reduction** :

$\left(\#\widetilde{M}^{(i)} < \#M^{(i)}\right) \wedge \left(M[i,j] = 0 \Rightarrow \widetilde{M}[i,j] = 0\right)$

At least one more zero entry. "Old" 0 entries are not modified.

(B) **Regularisation** : $\widetilde{M}[i,j]/M[i',j] = \widetilde{M}[i,j']/M[i',j']$.

More entries differing from the corresponding ones in another line by a common multiplicative factor than before.

Example (A,B): in A_3,

$$(16\ 8\ 4\ 2\ 1) + 2(1\ \ {-1}\ 1\ \ {-1}\ 1) \to \begin{matrix}(18 & \boxed{6\ 6} & 0\ 3) \\ (\ 1 & \boxed{1\ 1} & 1\ 1)\end{matrix}$$

Operations we count on for linear algebra

Linear combinations

$l_i \leftarrow (c_i \cdot l_i + c_j \cdot l_j)/d_i$, where c_i, c_j, d_i are "small" constants.

"small" actually means fixed: asymptotically small. Typically fits in 1 WORD.

Basic on long operands: linear operations

	$\lvert c_i \rvert$	$\lvert c_j \rvert$	d_i	cost
Add/Sub	1	1	1	`STEP`
l.c of first type	1	2^k	1	`STEP + (_1_2)`
	2^k	1	1	`STEP + (_1_2)`
l.c of second type	1	$\neq 2^k$	1	`STEP + (_1_X)`
	$\neq 2^k$	1	1	`STEP + (_1_X)`
Division by 2^k (shift)	1	0	2^k	`SHIFT`
Exact division	1	0	$\neq 2^k$	`DIV`

The Toom graph

Let $G = (V, E, w)$ the weighted graph such that

1. V is the set of matrices obtained by A_n with $\longrightarrow^*$ subject to criteria (A) and (B).
2. E is the set of edges such that $(M, \widetilde{M}) \in E \Leftrightarrow \widetilde{M}$ can be obtained by M by means of an admissible linear combination.

The Toom graph

Let $G = (V, E, w)$ the weighted graph such that

1. V is the set of matrices obtained by A_n with $\to^*$ subject to criteria (A) and (B).
2. E is the set of edges such that $(M, \widetilde{M}) \in E \Leftrightarrow \widetilde{M}$ can be obtained by M by means of an admissible linear combination.

Definition (weight function)

For $\varepsilon \in E$, $w(\varepsilon)$ is the cost of the corresponding linear combination. For a chain $\mathcal{C}$, $w(\mathcal{C}) = \sum_{\varepsilon \in \mathcal{C}} w(\varepsilon)$.

$$w(M) = \min_{\mathcal{C}(M,I)} \{w(\mathcal{C})\}$$

Example (Karatsuba graph): Let $(v_1 = \infty, v_2 = 1, v_3 = 0)$

$$\begin{array}{ccc}
\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \xrightarrow{\varepsilon_1} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\
\downarrow \varepsilon_2 & & \downarrow \varepsilon_3 \\
\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \xrightarrow{\varepsilon_4} & I
\end{array}$$

Example (Knuth graph): Let $(v_1 = \infty, v_2 = -1, v_3 = 0)$

$$\begin{array}{ccc}
\begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \xrightarrow{\varepsilon_1} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\
\downarrow \varepsilon_2 & & \downarrow \varepsilon_3 \\
\begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \xrightarrow{\varepsilon_4} & I
\end{array}$$

Heuristics for search pruning

We use a recursive function f to visit G, keeping some vertexes for some time to benefit from already made evaluations.

Heuristics for search pruning

We use a recursive function f to visit G, keeping some vertexes for some time to benefit from already made evaluations.

- We make **estimates** (from below) $e(M)$ of $w(M)$ by exploiting various heuristics (matrix support cardinality, determinant value, submatrices, etc).
- We introduce a **threshold** t (parameter for f) to avoid analysing not interesting subgraphs. If $e(M) > t$ the subgraph under M is not analysed (no better IS can be drawn from it).
- t is updated while f visits G: if $M \xrightarrow{\varepsilon} \widetilde{M}$ and $f(M,t)$ calls itself, then the recursive call is $f(\widetilde{M}, t - w(\varepsilon))$.

Heuristics for search pruning

We use a recursive function f to visit G, keeping some vertexes for some time to benefit from already made evaluations.

- We make **estimates** (from below) $e(M)$ of $w(M)$ by exploiting various heuristics (matrix support cardinality, determinant value, submatrices, etc).
- We introduce a **threshold** t (parameter for f) to avoid analysing not interesting subgraphs. If $e(M) > t$ the subgraph under M is not analysed (no better IS can be drawn from it).
- t is updated while f visits G: if $M \xrightarrow{\varepsilon} \widetilde{M}$ and $f(M, t)$ calls itself, then the recursive call is $f(\widetilde{M}, t - w(\varepsilon))$.

Heuristics for search pruning

We use a recursive function f to visit G, keeping some vertexes for some time to benefit from already made evaluations.

- We make **estimates** (from below) $e(M)$ of $w(M)$ by exploiting various heuristics (matrix support cardinality, determinant value, submatrices, etc).
- We introduce a **threshold** t (parameter for f) to avoid analysing not interesting subgraphs. If $e(M) > t$ the subgraph under M is not analysed (no better IS can be drawn from it).
- t is updated while f visits G: if $M \xrightarrow{\varepsilon} \widetilde{M}$ and $f(M, t)$ calls itself, then the recursive call is $f(\widetilde{M}, t - w(\varepsilon))$.

Toom-2.5 optimal IS

$A_{2.5}$ generated by $\{\infty, -1, 1, 0\}$, with $\det(A_{2.5}) = 2$.
A Toom-graph with 17 nodes was built. The weight is

$$4 \cdot \mathtt{STEP} + \mathtt{SHIFT}$$

$$A_{2.5} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{2-=3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[3-=1]{2\gg(1)} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[2-=4]{3-=2} I$$

There are 16 minimal equivalent IS.

Toom-3 optimal IS

A_3 generated by $\{\infty, 2, -1, 1, 0\}$, with $\det(A_3) = 12$.
The IS implemented in GMP 4.2.1 uses both criteria. Its weight is

$$w_{GMP} = 8 \cdot \mathtt{STEP} + \mathtt{DIV} + 2 \cdot \mathtt{SHIFT} + 2 \cdot (\_1\_2)$$

Toom-3 optimal IS

A_3 generated by $\{\infty, 2, -1, 1, 0\}$, with $\det(A_3) = 12$.
The IS implemented in GMP 4.2.1 uses both criteria. Its weight is

$$w_{GMP} = 8 \cdot \mathtt{STEP} + \mathtt{DIV} + 2 \cdot \mathtt{SHIFT} + 2 \cdot (\mathtt{\_1\_2})$$

The solution we found uses only criterion (A) and its weight is

$$w_{BZ} = 8 \cdot \mathtt{STEP} + \mathtt{DIV} + \mathtt{SHIFT} + \min(\mathtt{\_1\_X}, \mathtt{SHIFT}) + \mathtt{\_1\_2}$$

depending on which of $\mathtt{\_1\_X}$, $\mathtt{SHIFT}$ is smaller.

Toom-3 optimal IS, when $\mathtt{SHIFT} < \mathtt{\_1\_X}$

$$A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 16 & 8 & 4 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{2-=4} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 15 & 9 & 3 & 3 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{4=3-4} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 15 & 9 & 3 & 3 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{3-=5}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 15 & 9 & 3 & 3 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow[4\gg(1)]{2/=(3)} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 5 & 3 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{2-=3} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{2\gg(1)}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{3-=4} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow[3-=1]{2-=(2)1} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \xRightarrow{4-=2} I$$

Toom-3.5 (4 × 3 or 5 × 2 unbalanced multiplications)

$A_{3.5}$ generated by $\{\infty, 2, -2, 1, -1, 0\}$. The weight is

$$12 \cdot \mathtt{STEP} + 2 \cdot \mathtt{DIV} + 2 \cdot \mathtt{SHIFT} + 2 \cdot (\_1\_2)$$

$$A_{3.5} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 32 & 16 & 8 & 4 & 2 & 1 \\ -32 & 16 & -8 & 4 & -2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

One regularisation step (B) is needed.

Toom-4 $(4 \times 4$ or 5×3 or $6 \times 2)$

A_4 generated by $\left\{\infty, 2, 1, -1, \frac{1}{2}, -\frac{1}{2}, 0\right\}$. The weight is

$$18 \cdot \mathtt{STEP} + 3 \cdot \mathtt{DIV} + \mathtt{SHIFT} + \min\left(\mathtt{\_1\_X}, \mathtt{SHIFT}\right) + 2 \cdot (\mathtt{\_1\_X}) + 4 \cdot (\mathtt{\_1\_2})$$

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 \\ 1 & -2 & 4 & -8 & 16 & -32 & 64 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

One regularisation step (B) is used.

Toom-4.5 $(5 \times 4$ or 6×3 or $7 \times 2)$

$A_{4.5}$ generated by $\left\{\infty, -1, -2, \frac{1}{2}, 1, 2, -\frac{1}{2}, 0\right\}$. The weight is

$$22 \cdot \mathtt{STEP} + 4 \cdot \mathtt{DIV} + \mathtt{SHIFT} + 3 \cdot (\mathtt{\_1\_X}) + 6 \cdot (\mathtt{\_1\_2})$$

$$A_{4.5} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -128 & 64 & -32 & 16 & -8 & 4 & -2 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 & 128 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 1 & -2 & 4 & -8 & 16 & -32 & 64 & -128 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Toom-5 (5 × 5 or 6 × 4 or 7 × 3 or 8 × 2)

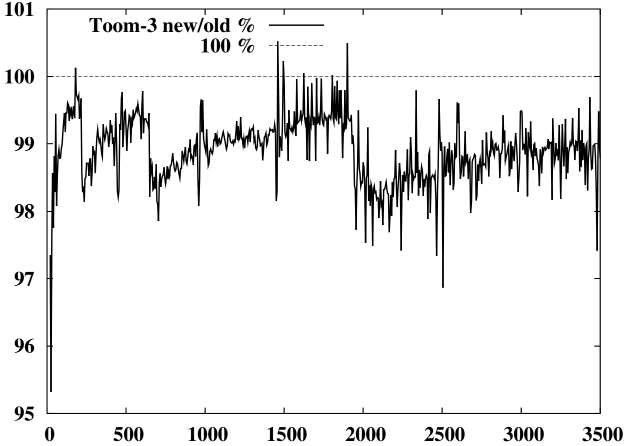
A_5 generated by $\left\{\infty, -2, \frac{1}{2}, 4, 2, -1, 1, -\frac{1}{2}, 0\right\}$. The weight is

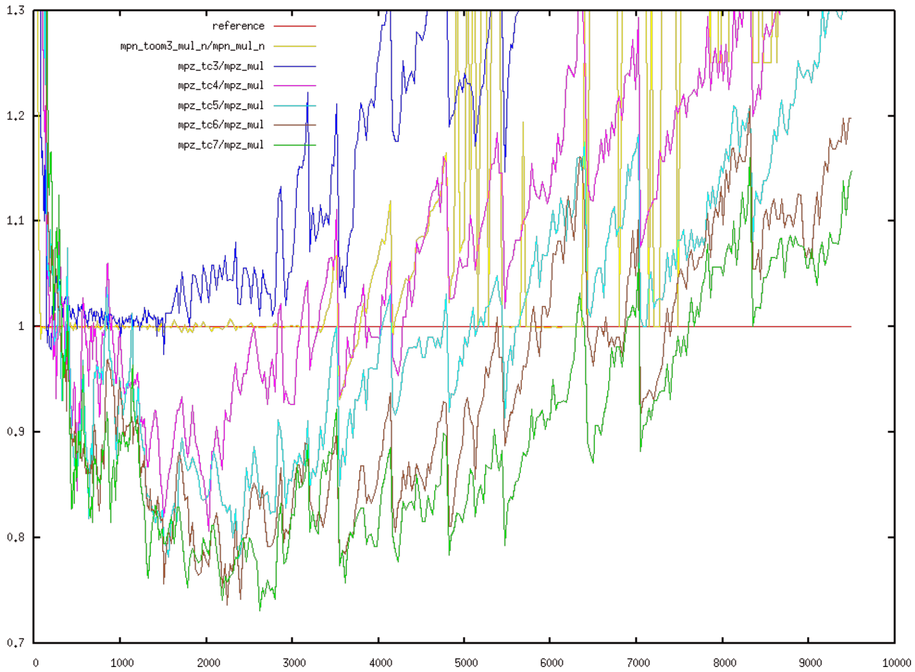
$$32 \cdot \mathtt{STEP} + 5 \cdot \mathtt{DIV} + 2 \cdot \mathtt{SHIFT} + 6 \cdot (\_1\_X) + 8 \cdot (\_1\_2)$$

$$A_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 256 & -128 & 64 & -32 & 16 & -8 & 4 & -2 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 & 64 & 128 & 256 \\ 4^8 & 4^7 & 4^6 & 4^5 & 256 & 64 & 16 & 4 & 1 \\ 256 & 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -2 & 4 & -8 & 16 & -32 & 64 & -128 & 256 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Toom-3 gain

We implemented new GMP code for Toom-3 with the new IS.




reference
mpn_toom3_mul_n/mpn_mul_n
mpz_tc3/mpz_mul
mpz_tc4/mpz_mul
mpz_tc5/mpz_mul
mpz_tc6/mpz_mul
mpz_tc7/mpz_mul
1.3
1.2
1.1
1
0.9
0.8
0.7
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000

Related results

Complete matrix inversion sequences for
Toom-3.5, Toom-4, Toom-4.5, Toom-5 in
What about Toom-Cook matrices optimality ?
Technical Report 605, Centro "Vito Volterra", Università di Roma "Tor Vergata", October 2006.
http://bodrato.it/papers/#CIVV2006.

Analysis for evaluation sequences,
result for Toom-3 in
Towards Optimal Toom-Cook Multiplication for Univariate and Multivariate Polynomials in Characteristic 2 and 0
presented at WAIFI 2007, Madrid, España, June 21-22, 2007.
http://bodrato.it/papers/#WAIFI2007.

That's all folks !

Thank you very much for your very kind attention

Questions ?

Presentation will be available on the web:
http://bodrato.it/papers/#ISSAC2007,