Multiplication Modulo A Triangular Set

Muhammad F.I. Chowdhury, Éric Schost
Dept. of Computer Science
University of Western Ontario, Canada

May 07, 2008

Triangular Set

Definition

A triangular set is a family of polynomial $\boldsymbol{T} = (T_1, T_2, \ldots, T_n)$ *in* $R[x_1, \ldots, x_n]$*, where*

- R *is our coefficient ring;*
- T_i *is in* $R[x_1, \ldots, x_i]$*;*
- T_i *is monic in* X_i*;*
- T_i *is reduced w.r.t.* $T_1, \ldots, T_{i-1}$.

Example

$$\begin{aligned} T_1(x_1) &= x_1^2 + 3x_1 \\ T_2(x_1, x_2) &= x_2^2 + x_2 x_1 \end{aligned}$$

Goal of this work

The goal of this work is to compute $C \equiv AB \mod T$ where A and B are two polynomials already reduced modulo T.

Example (continued)

$$\begin{aligned}
A &= x_1x_2 + x_2 + x_1 + 1 \\
B &= x_1x_2 + x_2 + x_1 + 1 \\
AB &= x_1^2x_2^2 + 2x_2^2x_1 + 2x_2x_1^2 + 4x_1x_2 + x_2^2 + 2x_2 + x_1^2 + 2x_1 + 1 \\
C &= -6x_2x_1 + 2x_2 - x_1 + 1
\end{aligned}$$

Complexity Measure

The complexity measure is $\delta = d_1 d_2 \ldots d_n$ (which is essentially the input and output size).

Theorem (Li, Moreno Maza, Schost)

The product $AB \mod T$ can be computed in time $\tilde{O}(4^n \delta)$.

(the notation $\tilde{O}$ hides logarithmic factors)

Theorem (Li, Moreno Maza, Schost)

Suppose that for all i, T_i is in $R[x_i]$. Then the product $AB \mod T$ can be computed in time

$$\tilde{O}(\delta \sum_{i=1}^{n} d_i).$$

Current work

Our contribution: extending the previous special case.

Theorem

Let T be a triangular set where, for all i:

- *T_i is in $R[x_i, x_{i-1}]$;*
- *$T_i = t_i(x_i) + q_i(x_{i-1})$;*
- *all t_i have the same degree d.*

Then the product $AB \mod T$ can be computed in time

$$\tilde{O}(d\delta).$$

Remarks

- The assumption that all d_i are equal simplifies the estimates.
- Combining this result with the $\tilde{O}(4^n\delta)$ bound, we can refine the cost to $\tilde{O}(\delta e^{\sqrt{\log \delta}})$.

Current work Contd.

Theorem

Let T be a triangular set where, for all i:

- T_i *is in* $R[x_i, x_{i-1}, \ldots, x_1]$;
- $T_i = t_i(x_i) + q_i(x_{i-1} \ldots x_1)$;
- *All* t_i *have the same degree* d.

Then the product $AB \mod T$ *can be computed in time*

$$\tilde{O}((2 - \frac{1}{d})^{n-1}\delta).$$

Application of modular arithmetic

Addition of algebraic numbers over $\mathbb{Z}/p\mathbb{Z}$.

This requires (in particular) multiplication modulo a triangular set T, where each T_i is in $\mathbb{Z}/p\mathbb{Z}[x_{i-1}, x_i]$ has degree p in x_i and 1 in x_{i-1}.

$$\begin{array}{rcl} T_1 & = & x_1^p \\ T_2 & = & x_2^p - x_1 \\ T_3 & = & x_3^p - x_2 \\ & \vdots & \\ T_n & = & x_n^p - x_{n-1} \end{array}$$

Our first theorem cover this case.

Application of modular arithmetic

A problem from cryptology, over $\mathbb{Z}/p\mathbb{Z}$.

This requires (in particular) multiplication modulo a triangular set T where each T_i is in $\mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_i]$ has degree p in x_i and $p-1, \ldots, p-1$ in $x_1, \ldots, x_{i-1}$.

$$\begin{aligned} T_1 &= x_1^p + x_1 + 1 \\ T_2 &= x_2^p + x_2 + x_1^{p-1} \\ T_3 &= x_3^p + x_3 + x_2^{p-1} x_1^{p-1} \\ &\vdots \\ T_n &= x_n^p + x_n + x_{n-1}^{p-1} \cdots x_1^{p-1} \end{aligned}$$

Our second theorem cover this case.

Nice case: when the roots are known

When all roots of $T_1, \ldots, T_n$ are known, the procedure is similar to the multiplication of multivariate polynomial using FFT.

Nice case: when the roots are known

When all roots of $T_1, \ldots, T_n$ are known, the procedure is similar to the multiplication of multivariate polynomial using FFT.

- Let A and B are two polynomials mod T, C is the product of AB mod T.
- C can be obtained by evaluation and interpolation at the roots of T.

Nice case: when the roots are known

When all roots of $T_1, \ldots, T_n$ are known, the procedure is similar to the multiplication of multivariate polynomial using FFT.

- Let A and B are two polynomials mod T, C is the product of AB mod T.
- C can be obtained by evaluation and interpolation at the roots of T.
- The evaluation of $A \mod T$ and $B \mod T$ can be done in time $\tilde{O}(\delta)$.

Nice case: when the roots are known

When all roots of $T_1, \ldots, T_n$ are known, the procedure is similar to the multiplication of multivariate polynomial using FFT.

- Let A and B are two polynomials mod T, C is the product of AB mod T.
- C can be obtained by evaluation and interpolation at the roots of T.
- The evaluation of $A \mod T$ and $B \mod T$ can be done in time $\tilde{O}(\delta)$.
- The multiplication is pairwise multiplication; the required time is $O(\delta)$.

Nice case: when the roots are known

When all roots of $T_1, \ldots, T_n$ are known, the procedure is similar to the multiplication of multivariate polynomial using FFT.

- Let A and B are two polynomials mod T, C is the product of AB mod T.
- C can be obtained by evaluation and interpolation at the roots of T.
- The evaluation of $A \mod T$ and $B \mod T$ can be done in time $\tilde{O}(\delta)$.
- The multiplication is pairwise multiplication; the required time is $O(\delta)$.
- The interpolation is essentially same as the evaluation which can be done in $\tilde{O}(\delta)$

Total: $\tilde{O}(\delta)$, optimal!

When the roots are unknown

In general, the roots are not known (they do no exist in R).

- Our approach consists in building another triangular set V with
$$V_i = \eta T_i + (1 - \eta) U_i,$$
where U_i has known roots (pairwise distinct).
- The root of V are series in η. We can compute them by Newton iteration, because the roots of U_i are known.
- If $\eta = 1$, then $V_i = T_i$.

Computing modulo the new triangular set

Instead of computing $C \equiv AB \mod T$ directly, we compute

- $C' = AB \mod V$ by evaluation and interpolation

Computing modulo the new triangular set

Instead of computing $C \equiv AB \mod T$ directly, we compute

- $C' = AB \mod V$ by evaluation and interpolation
- Substitute $\eta = 1$ in C'

This gives us $AB \mod T$.

Computing modulo the new triangular set

Instead of computing $C \equiv AB \mod T$ directly, we compute

- $C' = AB \mod V$ by evaluation and interpolation
- Substitute $\eta = 1$ in C'

This gives us $AB \mod T$.

Proposition

Let $r = deg(C', \eta)$, then the cost of the algorithm is $\tilde{O}(\delta r)$

Computing modulo the new triangular set

Instead of computing $C \equiv AB \mod T$ directly, we compute

- $C' = AB \mod V$ by evaluation and interpolation
- Substitute $\eta = 1$ in C'

This gives us $AB \mod T$.

Proposition

Let $r = deg(C', \eta)$, then the cost of the algorithm is $\tilde{O}(\delta r)$

Question: What will be the value of r?

Example of reduction

In general $r = \delta$, so we focus on special cases.

Example of reduction

In general $r = \delta$, so we focus on special cases.

Example

- The triangular set V is composed of:

$$\begin{aligned} V_1 &= x_1^3 - \eta x_1^2 - \eta x_1 - \eta \\ V_2 &= x_2^3 - \eta x_2^2 - \eta x_2 - \eta - \eta x_1^2 \\ V_3 &= x_3^3 - \eta x_3^2 - \eta x_3 - \eta - \eta x_2^2 \end{aligned}$$

- A and B are two polynomials $\bmod V$ in $R[x_1, x_2, x_3]$
- $C = AB \bmod V$ in $R[\eta][x_1, x_2, x_3]$.

Example of reduction contd.

Example (continued)

- The largest monomial of C, before reduction: $x_3^4 x_2^4 x_1^4$.
- A single reduction w.r.t. V_3:

$$\begin{aligned} x_3^4 x_2^4 x_1^4 &= x_3 x_3^3 x_2^4 x_1^4 \\ &= x_3 x_2^4 x_1^4 (\eta x_3^2 + \eta x_3 + \eta + \eta x_2^2) \quad \text{reduction w.r.t. } V_3 \\ &= \eta x_3^3 x_2^4 x_1^4 + \eta x_3^2 x_2^4 x_1^4 + \eta x_3 x_2^4 x_1^4 + \eta x_3 x_2^6 x_1^4 \end{aligned}$$

- The same process is repeated for $\eta x_3^3 x_2^4 x_1^4$

Example of reduction contd.

Example (continued)

- The monomial is $\eta x_3^3 x_2^4 x_1^4$.
- The reduction process:

$$\begin{aligned} \eta x_3^3 x_2^4 x_1^4 &= \eta x_2^4 x_1^4(\eta x_3^2 + \eta x_3 + \eta + \eta x_2^2) \quad \text{reduction w.r.t. } V_3 \\ &= \eta^2 x_3^2 x_2^4 x_1^4 + \eta^2 x_3 x_2^4 x_1^4 + \eta^2 x_2^4 x_1^4 + \eta^2 x_2^6 x_1^4 \end{aligned}$$

- Number of steps up to now: 2.
- The largest monomial after reducing w.r.t. V_3: $\eta^2 x_2^6 x_1^4$.

Example of reduction contd.

Example (continued)

- A single reduction w.r.t. V_2:

$$\begin{aligned}
\eta^2 x_1^4 x_2^6 &= \eta^2 x_1^4 x_2^3 x_2^3 \\
&= \eta^2 x_1^4 x_2^3 (\eta x_2^2 + \eta x_2 + \eta + \eta x_1^2) \quad \text{reduction w.r.t. } V_2 \\
&= \eta^3 x_1^4 x_2^5 + \eta^3 x_1^4 x_2^4 + \eta^3 x_1^4 x_2^3 + \eta^3 x_1^6 x_2^3
\end{aligned}$$

- This process gives us two alternative way to reduce C further.

Example contd.

The following tree structure describes the reduction more concisely.

Example contd.

The following tree structure describes the reduction more concisely.

$$\eta^2 x_1^4 x_2^6$$

Example contd.

The following tree structure describes the reduction more concisely.

$$\begin{tikzcd}
 & \eta^2 x_1^4 x_2^6 \arrow[dl] \arrow[dr] & \\
\eta^3 x_1^4 x_2^5 & & \eta^3 x_1^6 x_2^3
\end{tikzcd}$$

Example contd.

The following tree structure describes the reduction more concisely.

$$\begin{tikzcd}
 & & \eta^2 x_1^4 x_2^6 \arrow[dl] \arrow[dr] & & \\
 & \eta^3 x_1^4 x_2^5 \arrow[dl] \arrow[dr] & & \eta^3 x_1^6 x_2^3 \arrow[dl] \arrow[dr] & \\
\eta^4 x_1^4 x_2^4 & & \eta^4 x_1^6 x_2^2 & & \eta^4 x_1^8
\end{tikzcd}$$

Example contd.

The following tree structure describes the reduction more concisely.

$$
\begin{tikzcd}[column sep=small]
 & & & \eta^2 x_1^4 x_2^6 \arrow[dl] \arrow[dr] & & \\
 & & \eta^3 x_1^4 x_2^5 \arrow[dl] \arrow[dr] & & \eta^3 x_1^6 x_2^3 \arrow[dl] \arrow[dr] & \\
 & \eta^4 x_1^4 x_2^4 \arrow[dl] \arrow[dr] & & \eta^4 x_1^6 x_2^2 & & \eta^4 x_1^8 \\
\eta^5 x_1^4 x_2^3 & & \eta^5 x_1^6 x_2 & & &
\end{tikzcd}
$$

Example contd.

The following tree structure describes the reduction more concisely.

$$\begin{tikzcd}
 & & & & \eta^2 x_1^4 x_2^6 \arrow[dl] \arrow[dr] & & \\
 & & & \eta^3 x_1^4 x_2^5 \arrow[dl] \arrow[dr] & & \eta^3 x_1^6 x_2^3 \arrow[dl] \arrow[dr] & \\
 & & \eta^4 x_1^4 x_2^4 \arrow[dl] \arrow[dr] & & \eta^4 x_1^6 x_2^2 & & \eta^4 x_1^8 \\
 & \eta^5 x_1^4 x_2^3 \arrow[dl] \arrow[dr] & & \eta^5 x_1^6 x_2 & & & \\
 \eta^6 x_1^4 x_2^2 & & \eta^6 x_1^6 & & & &
\end{tikzcd}$$

Generalization

The previous example generalizes to

$$\begin{aligned}
V_1 &= x_1^{d_1} + c_{1,\ldots}(\eta) x_1^{d_1-1} + \cdots + c_{1,\ldots}(\eta) \\
V_2 &= x_2^{d_2} + c_{2,\ldots}(\eta) x_2^{d_2-1} + \cdots + c_{2,\ldots}(\eta) + c_{2,\ldots}(\eta) x_1^{d_1-1} + \cdots \\
&\vdots \\
V_n &= x_n^{d_n} + c_{n,\ldots}(\eta) x_n^{d_n-1} + \cdots + c_{n,\ldots}(\eta) + c_{n,\ldots}(\eta) x_{n-1}^{d_{n-1}-1} + \cdots\ ,
\end{aligned}$$

for some coefficients $c_{i,\ldots}(\eta)$ of degree 1.

Bound

The degree bound r will be:

- if $d_1 \leq d_2 \leq \cdots \leq d_{n-1} \leq d_n$

$$r \leq 2\sum_{i=1}^{n} d_i - 2$$

Bound

The degree bound r will be:

- if $d_1 \leq d_2 \leq \cdots \leq d_{n-1} \leq d_n$

$$r \leq 2\sum_{i=1}^{n} d_i - 2$$

- if $d_1 \geq d_2 \geq \cdots \geq d_{n-1} \geq d_n$

$$r \leq \sum_{i=2}^{n}(d_i - 1) + \sum_{i=2}^{n-1} i + n(d_1 - 1)$$

In particular, this gives our first theorem, when all d_i are equal.

Triangular set for 2nd case

Generalized triangular set for Theorem 2:

$$
\begin{aligned}
V_1 &= x_1^d + c_{1,\dots}(\eta)x_1^{d-1} + \cdots + c_{1,\dots}(\eta) \\
V_2 &= x_2^d + c_{2,\dots}(\eta)x_2^{d-1} + \cdots + c_{2,\dots}(\eta) + c_{2,\dots}(\eta)x_1^{d-1} + \cdots \\
&\vdots \\
V_n &= x_n^d + c_{n,\dots}(\eta)x_n^{d-1} + \cdots + c_{n,\dots}(\eta) + c_{n,\dots}(\eta)x_{n-1}^{d-1} \cdots x_1^{d-1} + \cdots
\end{aligned}
$$

for some coefficients $c_{i,\dots}(\eta)$ of degree 1.

Degree Changes in two direction:

Decrement of degrees for this case.

- Degrees in other variable remain same except x_i (when reducing w.r.t. V_i) which will be decreased by 1 in left direction
- Degrees in other variable increased by $(d-1)$ and decreased by d in x_i (when reducing w.r.t. V_i) in right direction

Degree Changes example:

If $d = 2$ and a monomial start with 3 variables having degrees $9, 9, 9$, then the reduction steps would be:

$$\begin{tikzcd}[column sep=tiny]
 & & & & & & & & 9,9,9 \arrow[dl] \arrow[dr] & & & & \\
 & & & & & & & 9,9,8 \arrow[dl] \arrow[dr] & & 10,10,7 \arrow[dl] \arrow[dr] & & & \\
 & & & & & & 9,9,7 \arrow[dl] \arrow[dr] & & 10,10,6 \arrow[dl] \arrow[dr] & & 11,11,5 \arrow[dl] \arrow[dr] & & \\
 & & & & & 9,9,6 \arrow[dl] \arrow[dr] & & 10,10,5 \arrow[dl] \arrow[dr] & & 11,11,4 \arrow[dl] \arrow[dr] & & 12,12,3 \arrow[dl] \arrow[dr] & \\
 & & & & 9,9,5 \arrow[dl] \arrow[dr] & & 10,10,4 \arrow[dl] \arrow[dr] & & 11,11,3 \arrow[dl] \arrow[dr] & & 12,12,2 \arrow[dl] \arrow[dr] & & 13,13,1 \\
 & & & 9,9,4 \arrow[dl] \arrow[dr] & & 10,10,3 \arrow[dl] \arrow[dr] & & 11,11,2 \arrow[dl] \arrow[dr] & & 12,12,1 & & 13,13,0 & \\
 & & 9,9,3 \arrow[dl] \arrow[dr] & & 10,10,2 \arrow[dl] \arrow[dr] & & 11,11,1 & & 12,12,0 & & & & \\
 & 9,9,2 \arrow[dl] \arrow[dr] & & 10,10,1 & & 11,11,0 & & & & & & & \\
9,9,1 & & 10,10,0 & & & & & & & & & &
\end{tikzcd}$$

Bound

The degree bound r will be:

- if $d_1 = d_2 = \cdots = d_{n-1} = d_n = d$

$$r \leq 2(2 - \frac{1}{d})^{n-1}$$

This gives our second theorem, when all d_i are equal.

Thanks