Fast and Small: Multiplying Polynomials without Extra Space

Daniel S. Roche

Symbolic Computation Group
School of Computer Science
University of Waterloo

CECM Day
SFU, Vancouver, 24 July 2009
Preliminaries

We study algorithms for univariate polynomial multiplication:

<table>
<thead>
<tr>
<th>The Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Given:</strong> A ring $R$, an integer $n$, and $f, g \in R[x]$ with degrees less than $n$</td>
</tr>
<tr>
<td><strong>Compute:</strong> Their product $f \cdot g \in R[x]$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Ring operations have unit cost</td>
</tr>
<tr>
<td>● Random reads from input, random reads/writes to output</td>
</tr>
<tr>
<td>● Space complexity determined by size of auxiliary storage</td>
</tr>
</tbody>
</table>
## Univariate Multiplication Algorithms

<table>
<thead>
<tr>
<th>Method</th>
<th>Time Complexity</th>
<th>Space Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classical Method</strong></td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td><strong>Divide-and-Conquer</strong></td>
<td>$O(n^{\log_2 3})$ or $O(n^{1.59})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td><strong>FFT-based</strong></td>
<td>$O(n \log n \log \log n)$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Karatsuba/Ofman ’63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cantor/Kaltofen ’91</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schönhage/Strassen ’71</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


## Univariate Multiplication Algorithms

<table>
<thead>
<tr>
<th>Method</th>
<th>Time Complexity</th>
<th>Space Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classical Method</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>Divide-and-Conquer</td>
<td>$O(n^{\log_2 3})$ or $O(n^{1.59})$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Karatsuba/Ofman ’63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FFT-based</td>
<td>$O(n \log n \log \log n)$</td>
<td>$O(n)$</td>
</tr>
<tr>
<td>Schönhage/Strassen ’71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cantor/Kaltofen ’91</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Goal: Keep time complexity the same, reduce space
The Evolution of Multiplication

Small and slow
The Evolution of Multiplication

Big and fast
The Evolution of Multiplication

Small and fast
Previous Work

- **Savage & Swamy 1979**: $O(n^2)$ time-space lower bound for straight line programs
- **Abrahamson 1985**: $O(n^2)$ time-space lower bound for branching programs
Previous Work

- **Savage & Swamy 1979**: $O(n^2)$ time-space lower bound for straight line programs.
- **Abrahamson 1985**: $O(n^2)$ time-space lower bound for branching programs.
- **Monagan 1993**: Importance of space efficiency for multiplication over $\mathbb{Z}_p[x]$.
- **Maeder 1993**: Bounds extra space for Karatsuba multiplication so that storage can be preallocated — about $2n$ extra memory cells required.
- **Thomé 2002**: Karatsuba multiplication for polynomials using $n$ extra memory cells.
Present Contributions

- New Karatsuba-like algorithm with $O(\log n)$ space
- New FFT-based algorithm with $O(1)$ space under certain conditions
- Implementations in C over $\mathbb{Z}/p\mathbb{Z}$
Standard Karatsuba Algorithm

Idea: Reduce one degree-\(2k\) multiplication to three of degree \(k\).

- Originally noticed by Gauss (multiplying complex numbers), rediscovered and formalized by Karatsuba & Ofman

Input: \(f, g \in \mathbb{R}[x]\) each with degree less than \(2k\).

Write \(f = f_0 + f_1 x^k\) and \(g = g_0 + g_1 x^k\).
Low-Space Karatsuba Algorithms

Version “0”

Read-Only Input Space:

- f₀₁
- f₁₁
- g₀
- g₁

Read/Write Output Space:

- (empty)
- (empty)
- (empty)
- (empty)

To Compute: \( f \cdot g \)
Low-Space Karatsuba Algorithms

Version “1”

1. The low-order coefficients of the output are initialized as $h$, and the product $f \cdot g$ is added to this.

To Compute: $f \cdot g + h$
Low-Space Karatsuba Algorithms

Version “2”

1. The low-order coefficients of the output are initialized as $h$, and the product $f \cdot g$ is added to this.

2. The first polynomial $f$ is given as a sum $f^{(0)} + f^{(1)}$.

Read-Only Input Space:

<table>
<thead>
<tr>
<th>f01</th>
<th>f11</th>
<th>g0</th>
<th>g1</th>
</tr>
</thead>
<tbody>
<tr>
<td>f00</td>
<td>f10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Read/Write Output Space:

| h0  | h1  | (empty) | (empty) |

To Compute: $(f^{(0)} + f^{(1)}) \cdot g + h$
Dirty Details

Restrict modulus to 29 bits to allow for delayed reductions

<table>
<thead>
<tr>
<th>In the Karatsuba step</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Only 4 values are added/subtracted in one position</td>
</tr>
<tr>
<td>• Delay reductions, perform two “corrections”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classical algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Switch over at $n \leq 32$ (determined experimentally)</td>
</tr>
<tr>
<td>• Perform arithmetic in double-precision long longs; delay reductions (a la Monagan)</td>
</tr>
</tbody>
</table>
Problem: code explosion

3 “versions” of algorithms (based on extra constraints)

×
Karatsuba or classical

×
odd-sized or even-sized operands

×
equal-sized operands or “one different”

Solution: Use “supermacros” in C:
Same file is included multiple times with some parameter values changed (crude form of code generation).
DFT-Based Multiplication

Input

Evaluation (DFT)

Pointwise multiplication

Interpolation (inverse DFT)

\[ f \times g \]
Simplifying Assumptions

From now on:

- $\deg f + \deg g < n = 2^k$ for some $k \in \mathbb{N}$
- The base ring $R$ contains a $2^k$-PRU $\omega$

That is, assume “virtual roots of unity” have already been found, and optimize from there.
Perform two $\frac{n}{2}$-DFTs followed by $\frac{n}{2}$ 2-DFTs:

- Write $f(x) = f_{\text{even}}(x^2) + x \cdot f_{\text{odd}}(x^2)$
  (i.e. $\deg f_{\text{even}}, \deg f_{\text{odd}} < n/2$)
- Compute DFT$_{\omega^2}(f_{\text{even}})$ and DFT$_{\omega^2}(f_{\text{odd}})$
- Compute each $f(\omega^i) = f_{\text{even}}(\omega^{2i}) + \omega \cdot f_{\text{odd}}(\omega^{2i})$

Make use of “butterfly circuit” for each size-2 DFT:
Example: 8-Way FFT

\[ f(\omega^0) \]
\[ f(\omega^4) \]
\[ f(\omega^2) \]
\[ f(\omega^6) \]
\[ f(\omega^1) \]
\[ f(\omega^5) \]
\[ f(\omega^3) \]
\[ f(\omega^7) \]
Reverted Binary Ordering

In-Place FFT permutes the ordering into reverted binary:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary 2</th>
<th>Reverted Binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000₂</td>
<td>000₂</td>
</tr>
<tr>
<td>1</td>
<td>001₂</td>
<td>001₂</td>
</tr>
<tr>
<td>2</td>
<td>010₂</td>
<td>010₂</td>
</tr>
<tr>
<td>3</td>
<td>011₂</td>
<td>011₂</td>
</tr>
<tr>
<td>4</td>
<td>100₂</td>
<td>100₂</td>
</tr>
<tr>
<td>5</td>
<td>101₂</td>
<td>101₂</td>
</tr>
<tr>
<td>6</td>
<td>110₂</td>
<td>110₂</td>
</tr>
<tr>
<td>7</td>
<td>111₂</td>
<td>111₂</td>
</tr>
</tbody>
</table>

**Problem**: Powers of $\omega$ are not accessed in order
Possible solutions:

- Precompute all powers of $\omega$ — too much space
- Perform steps out of order — terrible for cache
- Permute input before computing — costly
Alternate Formulation of FFT

Perform $\frac{n}{2}$ 2-DFTs followed by two $\frac{n}{2}$-DFTs

- Write $f = f_{\text{low}} + x^{n/2} \cdot f_{\text{high}}$
- Compute $f_0 = f_{\text{low}} + f_{\text{high}}$ and $f_1 = f_{\text{low}}(\omega x) - f_{\text{high}}(\omega x)$
- Compute each $f(\omega^2i) = f_0(\omega^2i)$ and $f(\omega^{2i+1}) = f_1(\omega^2i)$

Modified “butterfly circuit”:

```
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>\downarrow{a + b}</td>
<td>\downarrow{(a - b)\omega^i}</td>
</tr>
<tr>
<td>\uparrow{i}</td>
<td>\uparrow{i}</td>
</tr>
</tbody>
</table>
```

diagram
Example: 8-Way In-Place FFT (Alternate Formulation)
Folded Polynomials

Recall the basis for the “alternate” FFT formulation:

\[ f_0 = f_{\text{low}} + f_{\text{high}} \]
\[ f_1 = f_{\text{low}}(\omega x) - f_{\text{high}}(\omega x) \]

A generalization (recalling that \( n = 2^k \)):

**Definition (Folded Polynomials)**

\[ f_i = f(\omega^{2^{i-1}} x) \mod x^{2^k - 1} \]

**Theorem**

\[ f \left( \omega^{2^i(2j+1)} \right) = f_{i+1} (\omega^{2^i+1} j) \]

So by computing each \( f_i \) at all powers of \( \omega^i \), we get the values of \( f \) at all powers of \( \omega \).
Recursively Applying the Alternate Formulation

Example (Reverted Binary Ordering of 0, 1, ... , 15)

0, 8, 4, 12, 2, 10, 6, 14, 1, 9, 5, 13, 3, 11, 7, 15

$\text{DFT}_\omega(f)$ in binary reversed order can be computed by DFTs of $f_i$s:

$\text{DFT}_\omega(f) = \text{DFT}_{\omega^8}(f_3) \circ \text{DFT}_{\omega^4}(f_2) \circ \text{DFT}_{\omega^2}(f_1)$
FFT-Based Multiplication without Extra Space

Idea: Solve half of remaining problem at each iteration

Input

(f) (g) (empty)
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

![Diagram](image-url)
**FFT-Based Multiplication without Extra Space**

**Idea:** Solve half of remaining problem at each iteration

In-Place FFTs (alternate formulation)
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

**Pointwise Multiplication**
FFT-Based Multiplication without Extra Space

Idea: Solve half of remaining problem at each iteration

Folding

\[ f \rightarrow f_2 \quad g \rightarrow g_2 \quad DFT(f_1 \cdot g_1) \]
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

\[
f \quad \cdot \quad g
\]

In-Place FFTs (alternate formulation)

\[
\text{DFT}(f2) \quad \text{DFT}(g2) \quad \text{DFT}(f1\cdot g1)
\]
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

**Pointwise Multiplication**

\[ \text{DFT}(f) \quad \text{DFT}(f_2 \cdot g_2) \quad \text{DFT}(f_1 \cdot g_1) \]
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

\[
\text{DFT}(f \cdot g)
\]

\(k\) iterations
FFT-Based Multiplication without Extra Space

**Idea:** Solve half of remaining problem at each iteration

\[ f \cdot g \]

In-Place Reverse FFT (usual formulation)
Analysis

Time cost of the various stages:

- **Folding**: $O(n)$ cost times $\log n$ folds = $O(n \log n)$
- **FFTs**: $O(m \log m)$ for $m = n, n/2, n/4, \ldots, 1 = O(n \log n)$
- **Multiplications**: $n/2 + n/4 + \cdots + 1 = O(n)$

Total cost: $O(n \log n)$ time and $O(1)$ extra space when the following conditions hold:

- $n = \deg f + \deg g + 1$ is a power of 2
- $R$ contains an $n$-PRU $\omega$
Modular Arithmetic

Use floating-point Barrett reduction (from NTL):

- Pre-compute an approximation of $1/p$
- Given $a, b \in \mathbb{Z}_p$, compute an approximation of $q = \lfloor a \cdot b \cdot (1/p) \rfloor$
- Then $ab - qp$ equals $ab \% p$ plus or minus $p$.

The cost of this method:

- 2 double multiplications
- 2 int multiplications
- 1 int subtraction
- 3 conversions between int and double
- 2 “correction” steps to get exact result
  \[\rightarrow\text{ not necessary until the very end!}\]
Implementation Benchmarking

Details of tests:

- 2.5 GHz 64-bit Athalon, 256KB L1, 1MB L2, 2GB RAM
- $p = 167772161$ (28 bits)
- Comparing CPU time (in seconds) for the computation

Disclaimer

We are comparing apples to oranges.
Timing Benchmarks

![Graph showing timing benchmarks for Karatsuba-like and FFT-based methods over \( \log_2 n \).]
Future Directions

• Efficient implementation over \( \mathbb{Z} \) (GMP)

• Similar results for Toom-Cook 3-way or \( k \)-way

• What modulus bit restriction is “best”?

• Is completely in-place (overwriting input) possible?