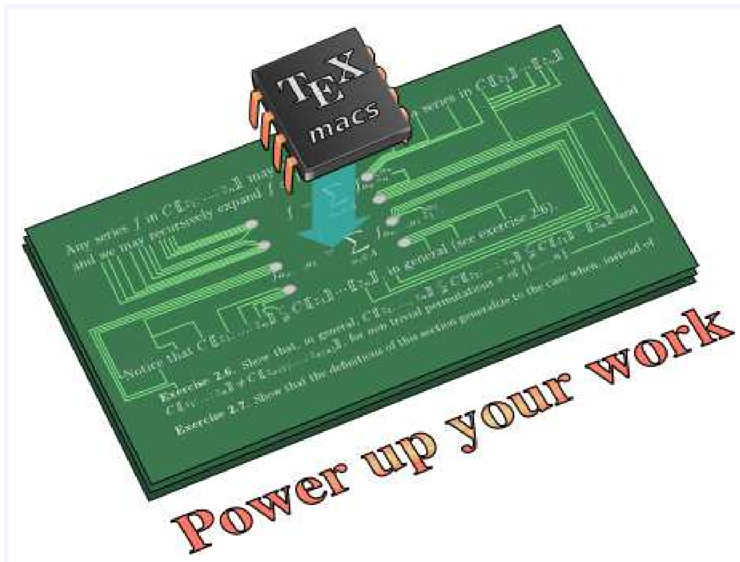
Faster relaxed multiplication

Joris van der Hoeven

CNRS, École polytechnique



ISSAC, 神戸市, 2014

`http://www.TeXmacs.org`

$\mathbb{A}$ an effective (not necessarily commutative) ring of coefficients

Polynomial multiplication

Given $f = f_0 + \cdots + f_{n-1} z^{n-1}$ and $g = g_0 + \cdots + g_{n-1} z^{n-1}$ in $\mathbb{A}[z]$, compute $f g$

$\mathsf{M}_{\mathbb{A}}(n) = O(n \log n \log \log n)$ [Schönhage-Strassen 1971, Cantor-Kaltofen 1991]

$\mathsf{M}_{\mathbb{A}}(n) = O(n \log n \, 8^{\log^* n})$ if $\operatorname{char} \mathbb{A} > 0$ [Harvey-vdH-Lecerf 2014 NEW]

"Zealous" (off-line) power series multiplication

Given power series $f, g \in \mathbb{A}[[z]]$ up to order $O(z^n)$, compute $f g$ up to order $O(z^n)$

Can clearly be done as well in time $\mathsf{M}_{\mathbb{A}}(n)$

"Relaxed" (on-line) power series multiplication

Add constraint that $(f g)_i$ should be printed as soon as $f_0, \ldots, f_i, g_0, \ldots, g_i$ are known

Question: what is the complexity $\mathsf{R}_{\mathbb{A}}(n)$ of relaxed multiplication?

$\mathbb{A}$ an effective (not necessarily commutative) ring of coefficients

Polynomial multiplication

Given $f = f_0 + \cdots + f_{n-1} z^{n-1}$ and $g = g_0 + \cdots + g_{n-1} z^{n-1}$ in $\mathbb{A}[z]$, compute $f g$

$\mathsf{M}_{\mathbb{A}}(n) = O(n \log n \log \log n)$ [Schönhage-Strassen 1971, Cantor-Kaltofen 1991]

$\mathsf{M}_{\mathbb{A}}(n) = O(n \log n \, 8^{\log^* n})$ if $\mathrm{char}\, \mathbb{A} > 0$ [Harvey-vdH-Lecerf 2014 NEW]

"Zealous" (off-line) power series multiplication

Given power series $f, g \in \mathbb{A}[[z]]$ up to order $O(z^n)$, compute $f g$ up to order $O(z^n)$

Can clearly be done as well in time $\mathsf{M}_{\mathbb{A}}(n)$

"Relaxed" (on-line) power series multiplication

Add constraint that $(f g)_i$ should be printed as soon as $f_0, \ldots, f_i, g_0, \ldots, g_i$ are known

Question: what is the complexity $\mathsf{R}_{\mathbb{A}}(n)$ of relaxed multiplication?

Exponentation

$$
\begin{aligned}
g &= \exp f = \textstyle\int f' \, g \\
g_n &= \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i) \, f_{n-i} \, g_i
\end{aligned}
$$

Example $f = z + z^2 + z^3 + \cdots$

$$g_0 = 1$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
	g_1							
	g_0							
		f_0'	f_1'	f_2'	f_3'	f_4'	f_5'	$\rightarrow$
		1	2	3	4	5	6	

Example and naive "lazy" algorithm

Exponentation

$$g = \exp f = \int f' \, g$$

$$g_n = \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i) \, f_{n-i} \, g_i$$

Example $f = z + z^2 + z^3 + \cdots$

$$g_0 = 1$$
$$g_1 = 1$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
	g_1							
1	g_0	1						
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Example and naive "lazy" algorithm

Exponentation

$$g = \exp f = \int f' g$$

$$g_n = \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i)\, f_{n-i}\, g_i$$

Example $f = z + z^2 + z^3 + \cdots$

$$g_0 = 1$$
$$g_1 = 1$$
$$g_2 = \frac{3}{2}$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
	g_2							
1	g_1	1						
1	g_0	1	2					
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Example and naive "lazy" algorithm

Exponentation

$$g = \exp f = \textstyle\int f' \, g$$

$$g_n = \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i) \, f_{n-i} \, g_i$$

Example $f = z + z^2 + z^3 + \cdots$

$$g_0 = 1$$
$$g_1 = 1$$
$$g_2 = \tfrac{3}{2}$$
$$g_3 = \tfrac{13}{6}$$

	$\uparrow$							
	g_5							
	g_4							
	g_3							
$\frac{3}{2}$	g_2	$\frac{3}{2}$						
1	g_1	1	2					
1	g_0	1	2	3				
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Example and naive "lazy" algorithm

Exponentation

$$
\begin{aligned}
g &= \exp f = \int f'\, g \\
g_n &= \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i)\, f_{n-i}\, g_i
\end{aligned}
$$

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24}
\end{aligned}
$$

	$\uparrow$							
	g_5							
	g_4							
$\frac{13}{6}$	g_3	$\frac{13}{6}$						
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3					
1	g_1	1	2	3				
1	g_0	1	2	3	4			
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Exponentation

$$g = \exp f = \int f'\, g$$

$$g_n = \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i)\, f_{n-i}\, g_i$$

Example $f = z + z^2 + z^3 + \cdots$

$$g_0 = 1$$
$$g_1 = 1$$
$$g_2 = \frac{3}{2}$$
$$g_3 = \frac{13}{6}$$
$$g_4 = \frac{73}{24}$$
$$g_5 = \frac{167}{40}$$

	$\uparrow$							
	g_5							
$\frac{73}{24}$	g_4	$\frac{73}{24}$						
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$				
1	g_1	1	2	3	4			
1	g_0	1	2	3	4	5		
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Exponentation

$$
\begin{aligned}
g &= \exp f = \int f' \, g \\
g_n &= \frac{1}{n} \sum_{i=0}^{n-1} (n+1-i) \, f_{n-i} \, g_i
\end{aligned}
$$

Example $f = z + z^2 + z^3 + \cdots$

$$
\begin{aligned}
g_0 &= 1 \\
g_1 &= 1 \\
g_2 &= \tfrac{3}{2} \\
g_3 &= \tfrac{13}{6} \\
g_4 &= \tfrac{73}{24} \\
g_5 &= \tfrac{167}{40} \\
g_6 &= \tfrac{4051}{720}
\end{aligned}
$$

	$\uparrow$							
$\frac{167}{40}$	g_5	$\frac{167}{40}$						
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$				
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6			
1	g_1	1	2	3	4	5		
1	g_0	1	2	3	4	5	6	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	$\rightarrow$
		1	2	3	4	5	6	

Fast “relaxed” algorithm

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
	g_2								
	g_1								
1	g_0	1							
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Fast “relaxed” algorithm

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
	g_2								
1	g_1	1							
1	g_0	1	2						
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Fast “relaxed” algorithm

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
	g_3								
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$					
1	g_1	1	2	3					
1	g_0	1	2	3					
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Fast “relaxed” algorithm

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
	g_5								
	g_4								
$\frac{13}{6}$	g_3	$\frac{13}{6}$							
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$					
1	g_1	1	2	3					
1	g_0	1	2	3	4				
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Fast “relaxed” algorithm

Anticipation ⇝ acceleration

	$\uparrow$								
	g_6								
	g_5								
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$			
1	g_1	1	2	3	4	5			
1	g_0	1	2	3	4	5			
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Fast “relaxed” algorithm

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
	g_6								
$\frac{167}{40}$	g_5	$\frac{167}{40}$							
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$					
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$					
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$			
1	g_1	1	2	3	4	5			
1	g_0	1	2	3	4	5	6		
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
$\frac{4051}{720}$	g_6	$\frac{4051}{720}$	$\frac{4051}{360}$	$\frac{4051}{240}$	$\frac{4051}{190}$	$\frac{4051}{144}$	$\frac{4051}{120}$	$\frac{28357}{720}$	
$\frac{167}{40}$	g_5	$\frac{167}{40}$	$\frac{167}{20}$	$\frac{501}{40}$	$\frac{167}{10}$	$\frac{167}{8}$	$\frac{501}{20}$	$\frac{1169}{40}$	
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$	$\frac{73}{6}$	$\frac{365}{24}$	$\frac{73}{4}$	$\frac{511}{24}$	
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$	$\frac{26}{3}$	$\frac{65}{6}$	13	$\frac{91}{6}$	
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$	9	$\frac{21}{2}$	
1	g_1	1	2	3	4	5	6	7	
1	g_0	1	2	3	4	5	6	7	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

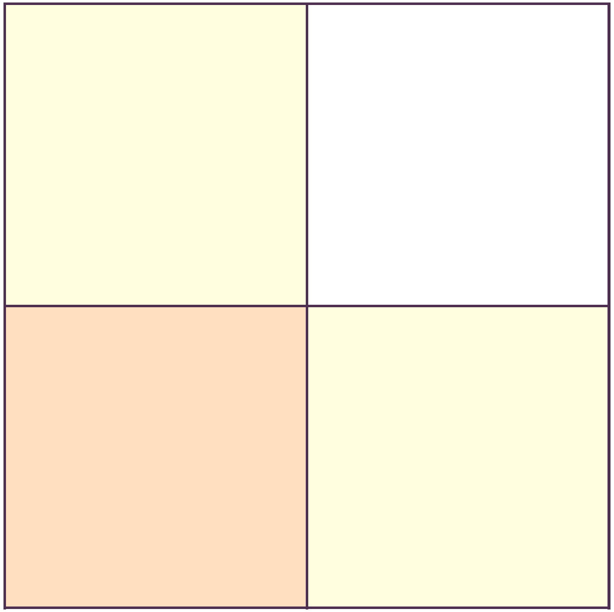
Anticipation $\rightsquigarrow$ acceleration

	$\uparrow$								
$\frac{4051}{720}$	g_6	$\frac{4051}{720}$	$\frac{4051}{360}$	$\frac{4051}{240}$	$\frac{4051}{190}$	$\frac{4051}{144}$	$\frac{4051}{120}$	$\frac{28357}{720}$	
$\frac{167}{40}$	g_5	$\frac{167}{40}$	$\frac{167}{20}$	$\frac{501}{40}$	$\frac{167}{10}$	$\frac{167}{8}$	$\frac{501}{20}$	$\frac{1169}{40}$	
$\frac{73}{24}$	g_4	$\frac{73}{24}$	$\frac{73}{12}$	$\frac{73}{8}$	$\frac{73}{6}$	$\frac{365}{24}$	$\frac{73}{4}$	$\frac{511}{24}$	
$\frac{13}{6}$	g_3	$\frac{13}{6}$	$\frac{13}{3}$	$\frac{13}{2}$	$\frac{26}{3}$	$\frac{65}{6}$	13	$\frac{91}{6}$	
$\frac{3}{2}$	g_2	$\frac{3}{2}$	3	$\frac{9}{2}$	6	$\frac{15}{2}$	9	$\frac{21}{2}$	
1	g_1	1	2	3	4	5	6	7	
1	g_0	1	2	3	4	5	6	7	
		f'_0	f'_1	f'_2	f'_3	f'_4	f'_5	f'_6	$\rightarrow$
		1	2	3	4	5	6	7	

$$\begin{aligned} \mathsf{R}_{\mathbb{A}}(n) &= O(2\,\mathsf{M}_{\mathbb{A}}(n/2) + 4\,\mathsf{M}_{\mathbb{A}}(n/4) + 8\,\mathsf{M}_{\mathbb{A}}(n/8) + \cdots) \\ &= O(\mathsf{M}_{\mathbb{A}}(n)\log n). \end{aligned}$$

[Fischer-Stockmeyer 1974, vdH 1997]

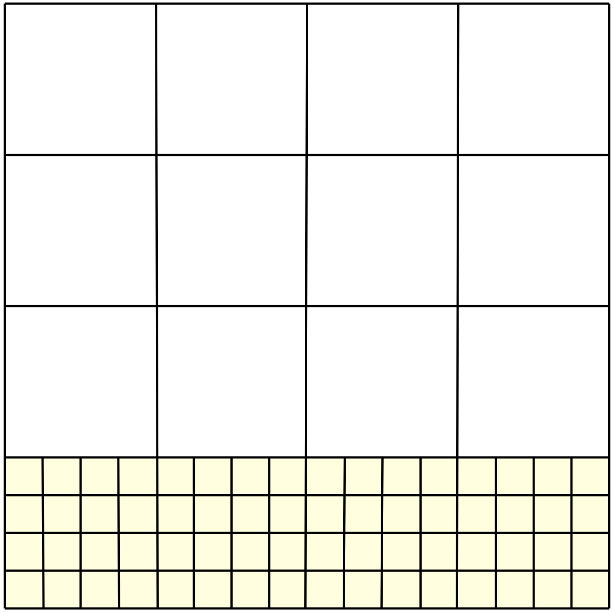
Relaxed $\rightsquigarrow$ Semi-relaxed products



Zealous
Semi-relaxed
Relaxed

Assume $\mathbb{A}$ contains a primitive 2^p-th root of unity for $2^p \geqslant 2n$

$\rightsquigarrow$ $\mathsf{M}(n) = \mathsf{M}_{\mathbb{A}}(n) = O(n \log n)$



$n = b\,m$, "block size" b, FFT-ed blocks in $\mathbb{A}^{2b}$

SR $n \times n$ product = m SR $b \times b$ products + one SR $m \times (m-1)$ product over $\mathbb{A}^{2b}$

$$\mathsf{S}(b\,m) \;=\; m\,\mathsf{S}(b) + 2\,b\,\mathsf{S}(m) + O(b\,m\log b)$$

Simple analysis: $b = m = \sqrt{n}$

$$\mathsf{S}(n) \;=\; 3\sqrt{n}\,\mathsf{S}(\sqrt{n}) + O(n\log n)$$

$\mathsf{S}(n) = n\,T(\log n)$

$$T(k) \;=\; 3\,T(k/2) + O(k)$$

Same recurrence as for Karatsuba's algorithm

$$\begin{aligned} T(k) &= O(k^{\log_2 3}) \\ \mathsf{R}(n) &= O(n\,(\log n)^{\log_2 3}) \end{aligned}$$

$$\mathsf{S}(b\,m) \;=\; m\,\mathsf{S}(b) + 2\,b\,\mathsf{S}(m) + O(b\,m\log b)$$

Optimal analysis [building on suggestion by referee]

$$\begin{aligned} m &= \exp\left(\frac{\log n}{\mathrm{e}^{\sqrt{2\log 2}\sqrt{\log\log n}}}\right) \\ b &= \frac{n}{m} \end{aligned}$$

Setting $\mathsf{S}(n) = n\log n\,T(\log n)$, one finds

$$\mathsf{R}(n) \;=\; \mathsf{R}_*(n) := O\!\left(n\log n\,\mathrm{e}^{\sqrt{2\log 2}\sqrt{\log\log n}}\sqrt{\log\log n}\right)$$

Case of "large" $\mathbb{A}$

Either $\begin{cases} \mathrm{char}\,\mathbb{A}=0 \text{ and } \mathbb{A} \text{ torsion-free as } \mathbb{Z}\text{-module and } \mathbb{A} \text{ admits division by integers} \\ \mathrm{char}\,\mathbb{A}>0 \text{ and } \mathbb{A} \text{ contains a geometric sequence of size } \geqslant n \end{cases}$

Evaluation on 2^p-th roots of unity $\rightsquigarrow$ Evaluation/interpolation on geometric sequence

Using [Bostan-Schost 2005], this can be done in time $O(\mathsf{M}_{\mathbb{A}}(b))$ for block size b

$$\begin{aligned} \mathsf{S}(b\,m) &= m\,\mathsf{S}(b)+2\,b\,\mathsf{S}(m)+O(m\,\mathsf{M}(b)) \\ \mathsf{R}(n) &= \mathsf{R}_{**}(n) := O\left(\mathsf{R}_{*}(n)\,\frac{\mathsf{M}(n)}{n\log n}\right) \end{aligned}$$

Case when $\mathbb{A}$ has small prime characteristic p

Rather compute over $\mathbb{B}=\mathbb{A}[x]/(P)$ with $\mathbb{F}_{p^k}=\mathbb{F}_p[x]/(P)$ and even $k\approx\log n/\log p$

Encode $k/2$ coefficients in $\mathbb{A}$ by one coefficient in $\mathbb{B}$

$$\begin{aligned} \mathsf{S}_{\mathbb{A}}(n) &\leqslant \frac{2\,n}{k}\,\mathsf{S}_{\mathbb{A}}\left(\frac{k}{2}\right)+\mathsf{S}_{\mathbb{B}}\left(\frac{2\,n}{k}\right)O(\mathsf{M}_{\mathbb{A}}(k)). \\ \mathsf{R}(n) &= \mathsf{R}_{***}(n) := O\left(\mathsf{R}_{**}(n)\,\frac{\mathsf{M}(\log n)}{\log n}\right) \end{aligned}$$

Case when $\mathbb{A}$ has small prime characteristic $s = p^r$

With $\mathbb{F}_{p^k} = \mathbb{F}_p[x]/(P)$ as above, monic $\tilde{P} \in (\mathbb{Z}/s\,\mathbb{Z})[x]$ with $\deg \tilde{P} = k$ and $\pi(\tilde{P}) = P$

$$\begin{array}{ccc} (\mathbb{Z}/s\,\mathbb{Z})[z]/(\tilde{P}) & \hookrightarrow & \mathbb{A}[z]/(\tilde{P}) \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{F}_p[z]/(P) & \hookrightarrow & (\mathbb{A}/p\,\mathbb{A})[z]/(P), \end{array}$$

Case when $\mathbb{A}$ has mixed characteristic $p_1^{r_1} \cdots p_l^{r_l}$

Use Chinese remaindering, as in [Cantor-Kaltofen 1991]

Summarizing

$$\mathsf{R}(n) = O(\mathsf{R}_*(n) \log\log n) \qquad \text{(characterstic 0)}$$
$$\mathsf{R}(n) = O(\mathsf{R}_*(n) \log\log n\, 64^{\log^* n}) \qquad \text{(otherwise)}$$

Relaxed p-adic multiplication [Fischer-Stockmeyer 1974, Berthomieu-vdH-Lecerf 2011]

$\mathsf{I}(n) = O(n \log n \, 8^{\log^* n})$: cost of n-bit integer multiplication [Harvey-vdH-Lecerf 2014 NEW]

Relaxed power series multiplication with bounded integer coefficients

$\mathcal{Z}_k = \{i \in \mathbb{Z} : |i| < 2^{k-1}\}$

$\mathsf{R}_{\mathbb{Z}}(n, k)$: cost of relaxed multiplication of $f, g \in \mathcal{Z}_k$ at order $O(z^n)$

$$\begin{aligned} \mathsf{R}_{\mathbb{Z}}(n,k) &= O(\mathsf{R}_{\mathbb{Z}/\pi^r\mathbb{Z}}(n)\, \mathsf{I}(\log_2(\pi^r))) \qquad (\pi^r > n\, 2^{2k}) \\ &= O(\mathsf{R}_{**}(n)\, \mathsf{I}(k + \log n)) \end{aligned}$$

Relaxed p-adic multiplication

Multiplying $f, g \in \mathbb{Z}_p$ at order $O(z^n)$ $\rightsquigarrow$ Multiplying $f, g \in \mathbb{Z}_{p^b}$ at order $O\left(z^{n/b}\right)$, $b = \frac{\log n}{\log p}$

$$\begin{aligned} \mathsf{S}_p(n) &\leqslant \tfrac{n}{b}\, \mathsf{S}_p(b) + \mathsf{S}_{p^b}\left(\tfrac{n}{b}\right) + O(n \log p) \\ \mathsf{S}_{p^b}\left(\tfrac{n}{b}\right) &= O\left(\mathsf{R}_{\mathbb{Z}}\left(\tfrac{n}{b}, \log_2(p^b)\right)\right) \\ \mathsf{R}_p(n) &= O((\mathsf{R}_{**}(n) \log p)\, \ell \log \ell) \\ \ell &= \log(\log n + \log p) \end{aligned}$$

Relaxed p-adic multiplication [Fischer-Stockmeyer 1974, Berthomieu-vdH-Lecerf 2011]

$\mathsf{I}(n) = O(n \log n \, 8^{\log^* n})$: cost of n-bit integer multiplication [Harvey-vdH-Lecerf 2014 NEW]

Relaxed power series multiplication with bounded integer coefficients

$\mathcal{Z}_k = \{i \in \mathbb{Z} \colon |i| < 2^{k-1}\}$

$\mathsf{R}_{\mathbb{Z}}(n, k)$: cost of relaxed multiplication of $f, g \in \mathcal{Z}_k$ at order $O(z^n)$

$$\begin{aligned} \mathsf{R}_{\mathbb{Z}}(n, k) &= O(\mathsf{R}_{\mathbb{Z}/\pi^r\mathbb{Z}}(n) \, \mathsf{I}(\log_2(\pi^r))) \qquad (\pi^r > n \, 2^{2k}) \\ &= O(\mathsf{R}_{**}(n) \, \mathsf{I}(k + \log n)) \end{aligned}$$

Relaxed p-adic multiplication

Multiplying $f, g \in \mathbb{Z}_p$ at order $O(z^n)$ $\rightsquigarrow$ Multiplying $f, g \in \mathbb{Z}_{p^b}$ at order $O\big(z^{n/b}\big)$, $b = \frac{\log n}{\log p}$

$$\begin{aligned} \mathsf{S}_p(n) &\leqslant \tfrac{n}{b} \, \mathsf{S}_p(b) + \mathsf{S}_{p^b}\big(\tfrac{n}{b}\big) + O(n \log p) \\ \mathsf{S}_{p^b}\big(\tfrac{n}{b}\big) &= O\big(\mathsf{R}_{\mathbb{Z}}\big(\tfrac{n}{b}, \log_2(p^b)\big)\big) \\ \mathsf{R}_p(n) &= O((\mathsf{R}_{**}(n) \log p) \, \ell \log \ell) \\ \ell &= \log(\log n + \log p) \end{aligned}$$