Fast multiple precision $\exp(x)$ with precomputations

Joris van der Hoeven, Fredrik Johansson
CNRS, École polytechnique, INRIA Bordeaux

ARITH 2024, Malaga, Spain

June 11, 2024

Main challenges

The problem

Given $x \in [0,1)$ and fixed $n \in \mathbb{N}$, compute $\exp x$ with a precision of n binary digits

Main challenges

The problem

Given $x \in [0,1)$ and fixed $n \in \mathbb{N}$, compute $\exp x$ with a precision of n binary digits

- Fast practical implementations for small, medium, and large n ?
- n fixed $\Longrightarrow$ we allow for lookup tables. Size ? Cost ?
- Complexity as a function of n ?
- How well does the theoretical complexity **model** practical complexity ?

Main challenges

The problem

Given $x \in [0,1)$ and fixed $n \in \mathbb{N}$, compute $\exp x$ with a precision of n binary digits

- Fast practical implementations for small, medium, and large n ?
- n fixed $\Longrightarrow$ we allow for lookup tables. Size ? Cost ?
- Complexity as a function of n ?
- How well does the theoretical complexity **model** practical complexity ?

Focus on $\exp$, but similar approach applies to $\log$, $\sin$, $\cos$, etc.

Complexity measures

$n \longrightarrow$ bit precision

$\mathsf{A}(n)$	cost to add two n-bit numbers
$\mathsf{M}(n)$	cost to multiply two n-bit numbers
$\mathsf{P}(n)$	cost to compute a "smooth" n-bit product of many small numbers
$\mathsf{E}(n)$	cost to multiply an n-bit exponential of $x \in [0,1)$

Complexity measures

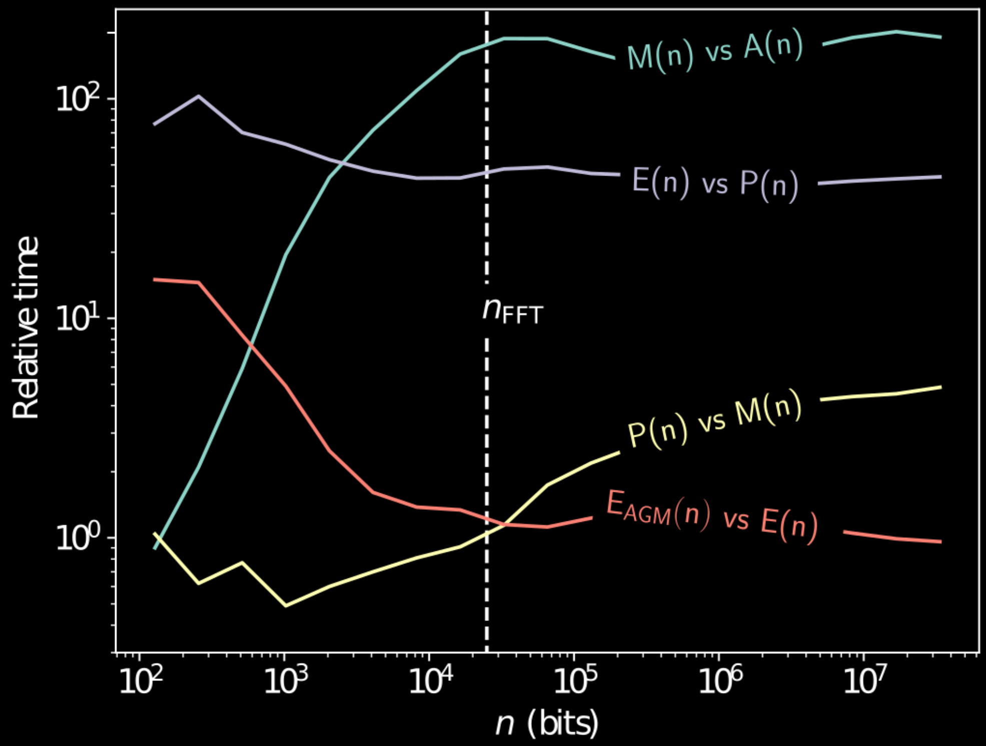
$n \longrightarrow$ bit precision

$\mathsf{A}(n)$	cost to add two n-bit numbers
$\mathsf{M}(n)$	cost to multiply two n-bit numbers
$\mathsf{P}(n)$	cost to compute a “smooth” n-bit product of many small numbers
$\mathsf{E}(n)$	cost to multiply an n-bit exponential of $x \in [0,1)$

In theory:

$$\begin{aligned} \mathsf{A}(n) &= O(n) \\ \mathsf{M}(n) &= O(n \log n) \\ \mathsf{P}(n) &= O(\mathsf{M}(n) \log n) \\ \mathsf{E}(n) &= O(\mathsf{M}(n) \log n) \end{aligned}$$

Practical complexity, currently in FLINT



General ideas for exponentiation

Argument reduction

$$x = x_1 + \cdots + x_k + \varepsilon$$
$$e^x = e^{x_1} \times \cdots \times e^{x_k} \times e^{\varepsilon}$$

$\longrightarrow$ multiple decomposition strategies

Taylor series expansion

$$e^{\varepsilon} \approx 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}$$

$\longrightarrow$ multiple strategies to evaluate the Taylor series

Bitwise reduction (naive)

$$x = 0.\ 0101\ \ 1001\ \ 0011\ \ 1011\ \ \cdots$$

Bitwise reduction (naive)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
&= 0.\ 0101\ 0000\ 0000\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 1001\ 0000\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 0000\ 0011\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 0000\ 0000\ 1011\ \cdots\ + \\
&\quad\ \cdots
\end{aligned}
$$

Bitwise reduction (naive)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
&= 0.\ 0101\ 0000\ 0000\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 1001\ 0000\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 0000\ 0011\ 0000\ \cdots\ + \\
&\quad\ 0.\ 0000\ 0000\ 0000\ 1011\ \cdots\ + \\
&\quad\ \cdots
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{e}^x &= 1.\ 0101\ 1101\ 1110\ 1001\ \cdots\ \times \\
&\quad\ 1.\ 0000\ 1001\ 0010\ 1000\ \cdots\ \times \\
&\quad\ 1.\ 0000\ 0000\ 0011\ 0000\ \cdots\ \times \\
&\quad\ 1.\ 0000\ 0000\ 0000\ 1011\ \cdots\ \times \\
&\quad\ \cdots
\end{aligned}
$$

Bitwise reduction (CORDIC, BKM)

$$x = 0.\ 0101\ 1001\ 0011\ 1011\ \cdots$$

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000
\end{aligned}
$$

Bitwise reduction (CORDIC, BKM)

$$\begin{aligned} x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\ x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\ x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000 \end{aligned}$$

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\
x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000\ 1100\ 1100\ \cdots \\
x_3 := x_2 - \log(1.\ 0000\ 0000\ 1100) &= 0.\ 0000\ 0000\ 0000
\end{aligned}
$$

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\
x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000\ 1100\ 1100\ \cdots \\
x_3 := x_2 - \log(1.\ 0000\ 0000\ 1100) &= 0.\ 0000\ 0000\ 0000\ 1101\ \cdots \\
x_4 := x_3 - \log(1.\ 0000\ 0000\ 0000\ 1101) &= 0.\ 0000\ 0000\ 0000\ 0000\ \cdots
\end{aligned}
$$

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\
x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000\ 1100\ 1100\ \cdots \\
x_3 := x_2 - \log(1.\ 0000\ 0000\ 1100) &= 0.\ 0000\ 0000\ 0000\ 1101\ \cdots \\
x_4 := x_3 - \log(1.\ 0000\ 0000\ 0000\ 1101) &= 0.\ 0000\ 0000\ 0000\ 0000\ \cdots
\end{aligned}
$$

$$
x \approx 1.\,0110 \times 1.\,0000\,0111 \times 1.\,0000\,0000\,1100 \times 1.\,0000\,0000\,0000\,1101
$$

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\
x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000\ 1100\ 1100\ \cdots \\
x_3 := x_2 - \log(1.\ 0000\ 0000\ 1100) &= 0.\ 0000\ 0000\ 0000\ 1101\ \cdots \\
x_4 := x_3 - \log(1.\ 0000\ 0000\ 0000\ 1101) &= 0.\ 0000\ 0000\ 0000\ 0000\ \cdots
\end{aligned}
$$

$$x \approx 1.\,0110 \times 1.\,0000\,0111 \times 1.\,0000\,0000\,1100 \times 1.\,0000\,0000\,0000\,1101$$

$\longrightarrow$ “Shift and add”

Bitwise reduction (CORDIC, BKM)

$$
\begin{aligned}
x &= 0.\ 0101\ 1001\ 0011\ 1011\ \cdots \\
x_1 := x - \log(1.\ 0110) &= 0.\ 0000\ 0111\ 1011\ 0100\ \cdots \\
x_2 := x_1 - \log(1.\ 0000\ 0111) &= 0.\ 0000\ 0000\ 1100\ 1100\ \cdots \\
x_3 := x_2 - \log(1.\ 0000\ 0000\ 1100) &= 0.\ 0000\ 0000\ 0000\ 1101\ \cdots \\
x_4 := x_3 - \log(1.\ 0000\ 0000\ 0000\ 1101) &= 0.\ 0000\ 0000\ 0000\ 0000\ \cdots
\end{aligned}
$$

$$x \approx 1.\,0110 \times 1.\,0000\,0111 \times 1.\,0000\,0000\,1100 \times 1.\,0000\,0000\,0000\,1101$$

$\longrightarrow$ "Shift and add" $\longrightarrow$ "Shift and FMA"

Complexity analysis

Reduction $x \longrightarrow \varepsilon$ with $\varepsilon < 2^{-r}$

m-bitwise

	Naive	**Shift and FMA**
Time	$\frac{r}{m}\mathsf{M}(n)$	$\frac{3r}{m}\mathsf{A}(n)$
Space	$\frac{2^m}{m}rn$	$\frac{2^m}{m}rn$

Diophantine approximation (Shönhage, Johansson)

$$x = 0.11062024$$

Diophantine approximation (Shönhage, Johansson)

$$x = 0.11062024$$

$$x \approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11$$

Diophantine approximation (Shönhage, Johansson)

$$
\begin{aligned}
x &= 0.11062024 \\
x &\approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11 \\
\exp x &\approx 2^{-33} \times 3^{-120} \times 5^{177} \times 7^{49} \times 11^{-94}
\end{aligned}
$$

Diophantine approximation (Shönhage, Johansson)

$$x = 0.11062024$$

$$x \approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11$$

$$\exp x \approx 2^{-33} \times 3^{-120} \times 5^{177} \times 7^{49} \times 11^{-94}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & 1 & 1 \\ 1 & 2 & -3 & 1 & 0 \\ -3 & 4 & -2 & -2 & 2 \\ -2 & 2 & 2 & -7 & 4 \\ -18 & -3 & 22 & 1 & -9 \end{pmatrix} \begin{pmatrix} \log 2 \\ \log 3 \\ \log 5 \\ \log 7 \\ \log 11 \end{pmatrix} \approx \begin{pmatrix} 0.69314718 \\ 0.18232156 \\ 0.02631731 \\ 0.00796817 \\ 0.00010204 \\ 0.00001609 \\ 0.00000065 \end{pmatrix} =: \begin{pmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \end{pmatrix}$$

Diophantine approximation (Shönhage, Johansson)

$$\begin{aligned} x &= 0.11062024 \\ x &\approx -33\log 2 - 120\log 3 + 177\log 5 + 49\log 7 - 94\log 11 \\ \exp x &\approx 2^{-33}\times 3^{-120}\times 5^{177}\times 7^{49}\times 11^{-94} \end{aligned}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & 1 & 1 \\ 1 & 2 & -3 & 1 & 0 \\ -3 & 4 & -2 & -2 & 2 \\ -2 & 2 & 2 & -7 & 4 \\ -18 & -3 & 22 & 1 & -9 \end{pmatrix} \begin{pmatrix} \log 2 \\ \log 3 \\ \log 5 \\ \log 7 \\ \log 11 \end{pmatrix} \approx \begin{pmatrix} 0.69314718 \\ 0.18232156 \\ 0.02631731 \\ 0.00796817 \\ 0.00010204 \\ 0.00001609 \\ 0.00000065 \end{pmatrix} =: \begin{pmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \end{pmatrix}$$

$$x := 0.11062024 \approx 4\,\ell_3$$

Diophantine approximation (Shönhage, Johansson)

$$x = 0.11062024$$

$$x \approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11$$

$$\exp x \approx 2^{-33} \times 3^{-120} \times 5^{177} \times 7^{49} \times 11^{-94}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & 1 & 1 \\ 1 & 2 & -3 & 1 & 0 \\ -3 & 4 & -2 & -2 & 2 \\ -2 & 2 & 2 & -7 & 4 \\ -18 & -3 & 22 & 1 & -9 \end{pmatrix} \begin{pmatrix} \log 2 \\ \log 3 \\ \log 5 \\ \log 7 \\ \log 11 \end{pmatrix} \approx \begin{pmatrix} 0.69314718 \\ 0.18232156 \\ 0.02631731 \\ 0.00796817 \\ 0.00010204 \\ 0.00001609 \\ 0.00000065 \end{pmatrix} =: \begin{pmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \end{pmatrix}$$

$$x - 4\,\ell_3 \approx 0.005351 \approx \ell_4$$

Diophantine approximation (Shönhage, Johansson)

$$
\begin{aligned}
x &= 0.11062024 \\
x &\approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11 \\
\exp x &\approx 2^{-33} \times 3^{-120} \times 5^{177} \times 7^{49} \times 11^{-94}
\end{aligned}
$$

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
1 & 1 & -1 & 0 & 0 \\
0 & -1 & -2 & 1 & 1 \\
1 & 2 & -3 & 1 & 0 \\
-3 & 4 & -2 & -2 & 2 \\
-2 & 2 & 2 & -7 & 4 \\
-18 & -3 & 22 & 1 & -9
\end{pmatrix}
\begin{pmatrix}
\log 2 \\ \log 3 \\ \log 5 \\ \log 7 \\ \log 11
\end{pmatrix}
\approx
\begin{pmatrix}
0.69314718 \\ 0.18232156 \\ 0.02631731 \\ 0.00796817 \\ 0.00010204 \\ 0.00001609 \\ 0.00000065
\end{pmatrix}
=:
\begin{pmatrix}
\ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7
\end{pmatrix}
$$

$$
x \approx 4\,\ell_3 + \ell_4 - 26\,\ell_5 + 2\,\ell_6 + 6\,\ell_7
$$

Diophantine approximation (Shönhage, Johansson)

$$x = 0.11062024$$
$$x \approx -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11$$
$$\exp x \approx 2^{-33} \times 3^{-120} \times 5^{177} \times 7^{49} \times 11^{-94}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & 1 & 1 \\ 1 & 2 & -3 & 1 & 0 \\ -3 & 4 & -2 & -2 & 2 \\ -2 & 2 & 2 & -7 & 4 \\ -18 & -3 & 22 & 1 & -9 \end{pmatrix} \begin{pmatrix} \log 2 \\ \log 3 \\ \log 5 \\ \log 7 \\ \log 11 \end{pmatrix} \approx \begin{pmatrix} 0.69314718 \\ 0.18232156 \\ 0.02631731 \\ 0.00796817 \\ 0.00010204 \\ 0.00001609 \\ 0.00000065 \end{pmatrix} =: \begin{pmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \end{pmatrix}$$

$$x \approx 4\,\ell_3 + \ell_4 - 26\,\ell_5 + 2\,\ell_6 + 6\,\ell_7$$
$$= -33 \log 2 - 120 \log 3 + 177 \log 5 + 49 \log 7 - 94 \log 11$$

Complexity analysis

Reduction $x \longrightarrow \varepsilon$ with $\varepsilon < 2^{-r}$

using m prime numbers $p_1, \ldots, p_m$

Complexity analysis

Reduction $x \longrightarrow \varepsilon$ with $\varepsilon < 2^{-r}$

using m prime numbers $p_1, \ldots, p_m$

Optimum $\quad m \;\approx\; \frac{\log 2}{2} r$

Complexity analysis

Reduction $x \longrightarrow \varepsilon$ with $\varepsilon < 2^{-r}$

using m prime numbers $p_1, \ldots, p_m$

Optimum $\quad m \approx \frac{\log 2}{2} r$

$$\text{Time} \quad 1.4\, r\, \mathsf{A}(n) + \mathsf{P}(\overbrace{\mathrm{e}^3 m^2 \log_2 m}^{\leqslant n}) + \mathsf{M}(n)$$

$$\text{Space} \quad m\, n$$

Complexity analysis

Reduction $x \longrightarrow \varepsilon$ with $\varepsilon < 2^{-r}$

using m prime numbers $p_1, \ldots, p_m$

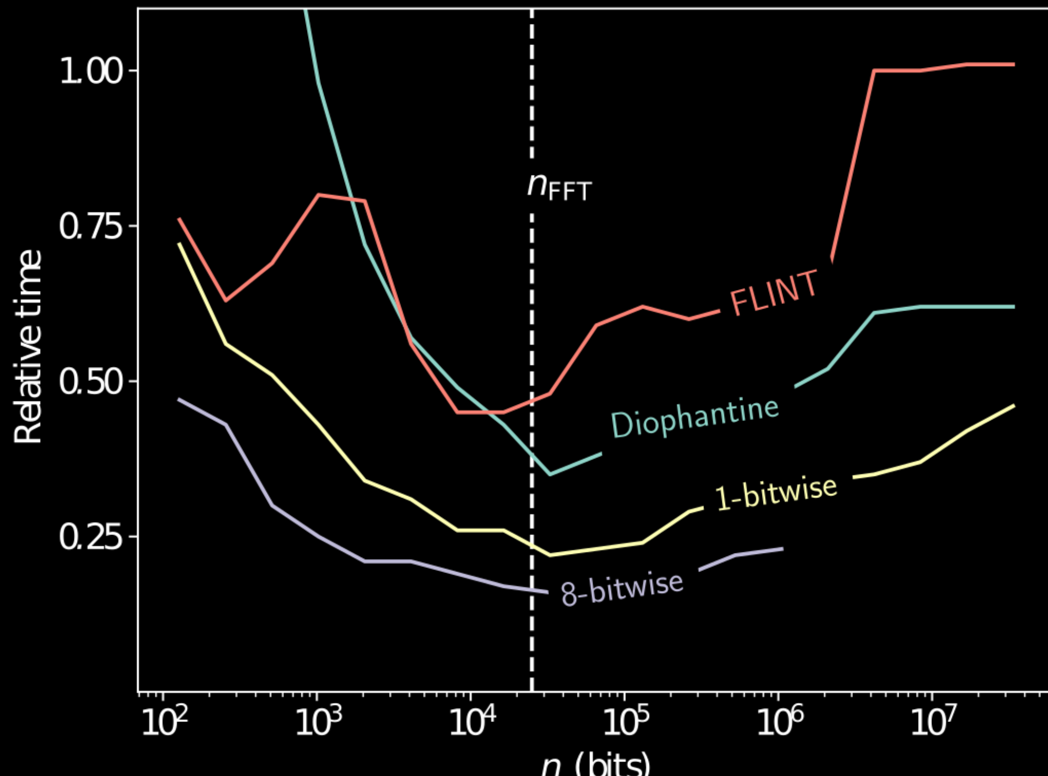
Optimum $\quad m \;\approx\; \frac{\log 2}{2} r$

$$\text{Time} \quad 1.4\, r\, \mathsf{A}(n) + \mathsf{P}(\overbrace{\mathrm{e}^3 m^2 \log_2 m}^{\leqslant n}) + \mathsf{M}(n)$$

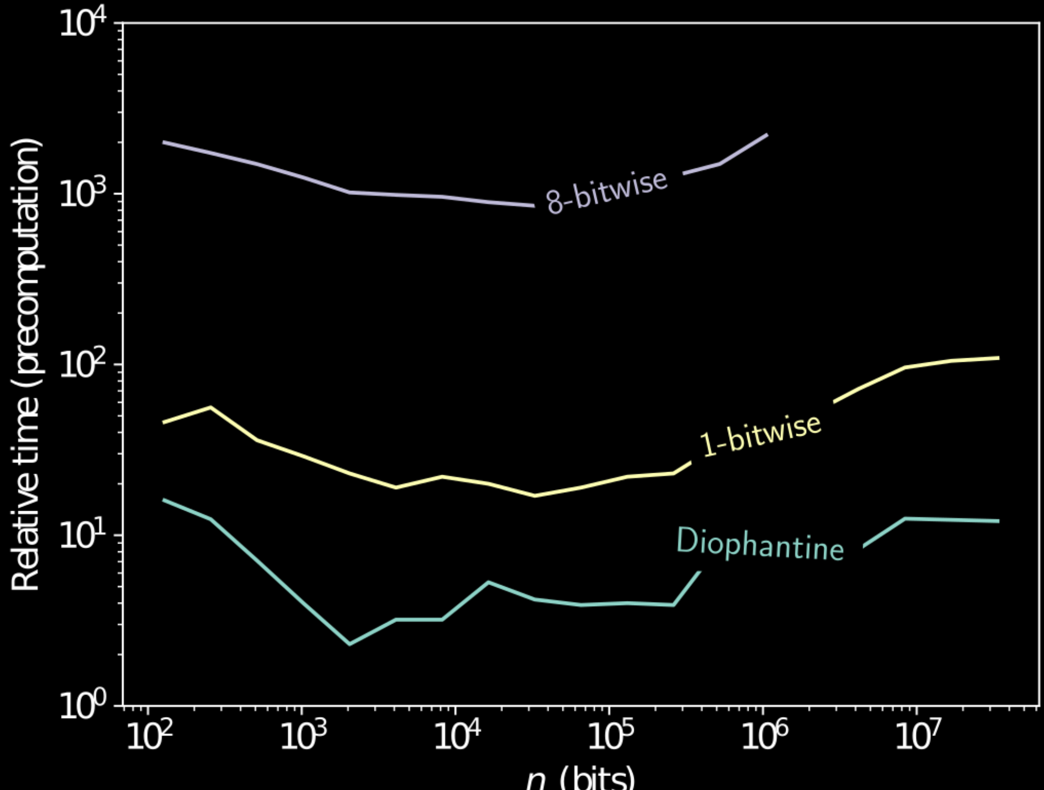
$$\text{Space} \quad m\, n$$

Optimum $\quad r \;\approx\; 2.9\, m \;\approx\; 0.64 \sqrt{\frac{n}{\log_2 n}}$

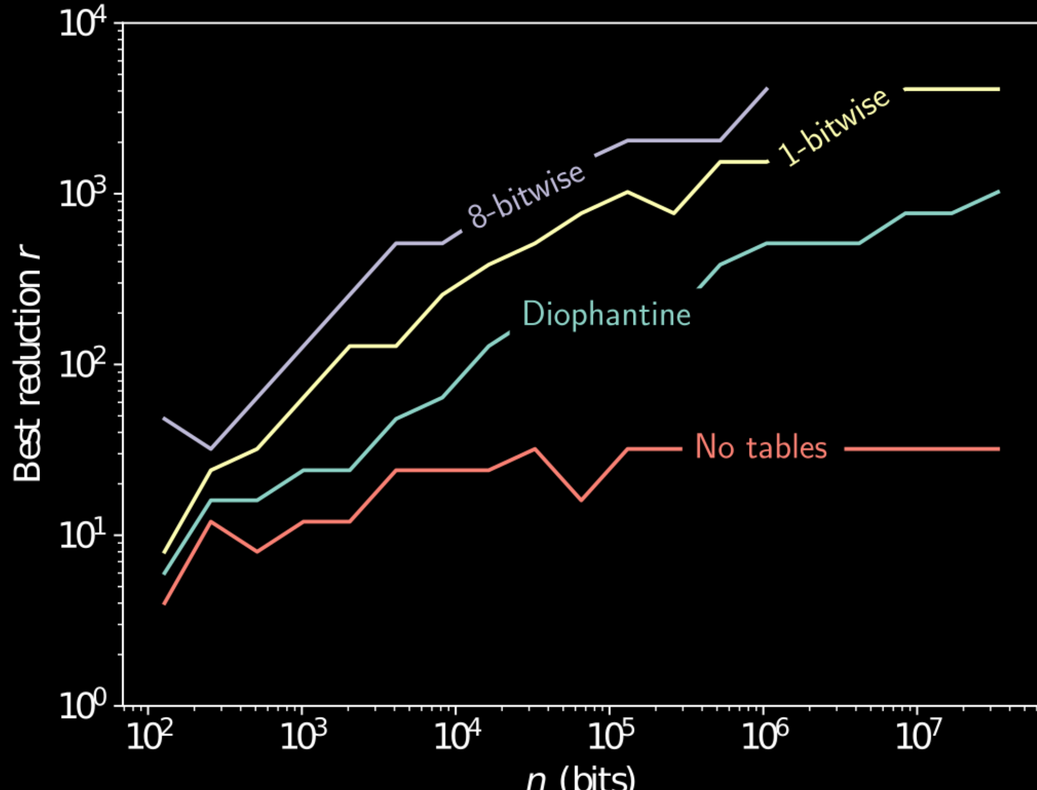
Overall timings w.r.t. squaring + Taylor series



Cost of precomputations



Best reduction threshold r



Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Horner's method $\frac{n}{r}\mathsf{M}(n)$

Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Horner's method $\frac{n}{r}\mathsf{M}(n)$

Hyperbolic sines $\frac{n}{2r}\mathsf{M}(n)$

$$\operatorname{sh}\varepsilon = \varepsilon + \tfrac{1}{6}\varepsilon^3 + \cdots + \tfrac{1}{(2N-1)!}\varepsilon^{2N-1}, \qquad N \approx \tfrac{n}{2r}$$

$$= \frac{e^{\varepsilon} - e^{-\varepsilon}}{2}$$

Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Horner's method $\frac{n}{r}\mathsf{M}(n)$

Hyperbolic sines $\frac{n}{2r}\mathsf{M}(n)$

$$\operatorname{sh}\varepsilon = \varepsilon + \frac{1}{6}\varepsilon^3 + \cdots + \frac{1}{(2N-1)!}\varepsilon^{2N-1}, \qquad N \approx \frac{n}{2r}$$

$$e^{\varepsilon} = \operatorname{sh}\varepsilon + \sqrt{1 + \operatorname{sh}^2\varepsilon}$$

Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Horner's method $\frac{n}{r}\mathsf{M}(n)$

Hyperbolic sines $\frac{n}{2r}\mathsf{M}(n)$

$$\operatorname{sh}\varepsilon = \varepsilon + \tfrac{1}{6}\varepsilon^3 + \cdots + \tfrac{1}{(2N-1)!}\varepsilon^{2N-1}, \qquad N \approx \tfrac{n}{2r}$$

$$e^{\varepsilon} = \operatorname{sh}\varepsilon + \sqrt{1 + \operatorname{sh}^2\varepsilon}$$

Curiosity: generalization with asymptotic complexity $\frac{n}{3r}\mathsf{M}(n)$

Taylor series

$$e^{\varepsilon} = 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \cdots + \frac{1}{(N-1)!}\varepsilon^{N-1}, \qquad N \approx \frac{n}{r}$$

Horner's method $\frac{n}{r}\mathrm{M}(n)$

Hyperbolic sines $\frac{n}{2r}\mathrm{M}(n)$

$$\operatorname{sh}\varepsilon = \varepsilon + \tfrac{1}{6}\varepsilon^3 + \cdots + \tfrac{1}{(2N-1)!}\varepsilon^{2N-1}, \qquad N \approx \tfrac{n}{2r}$$

$$e^{\varepsilon} = \operatorname{sh}\varepsilon + \sqrt{1 + \operatorname{sh}^2\varepsilon}$$

Curiosity: generalization with asymptotic complexity $\frac{n}{3r}\mathrm{M}(n)$

Rectangular splitting $c\sqrt{\frac{n}{r}}\mathrm{M}(n), \qquad \left(\tfrac{2}{3} \leqslant c \leqslant \tfrac{5}{3}\right)$

Binary splitting, bit burst

$$x = 0.\ 01\ 01\ 1011\ 01001001\ 0000111010111010\ 01001010010100111001010010110010$$

$$\varepsilon = 0.\ 00\ 00\ 0000\ 01001001$$

$$e^{\varepsilon} \approx 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \frac{1}{6}\varepsilon^3 + \frac{1}{24}\varepsilon^4 + \frac{1}{120}\varepsilon^5 + \frac{1}{720}\varepsilon^6 + \frac{1}{5040}\varepsilon^7$$

Binary splitting, bit burst

$$x = 0.\ 01\ 01\ 1011\ 01001001\ 0000111010111010\ 01001010010100111001010010110010$$

$$\varepsilon = 0.\ 00\ 00\ 0000\ 01001001$$

$$e^{\varepsilon} \approx 1 + \varepsilon + \frac{1}{2}\varepsilon^2 + \frac{1}{6}\varepsilon^3 + \frac{1}{24}\varepsilon^4 + \frac{1}{120}\varepsilon^5 + \frac{1}{720}\varepsilon^6 + \frac{1}{5040}\varepsilon^7$$

$1+\varepsilon$ $\quad 3+\varepsilon$ $\quad 5+\varepsilon$ $\quad 7+\varepsilon$ $\quad \approx$16 bits

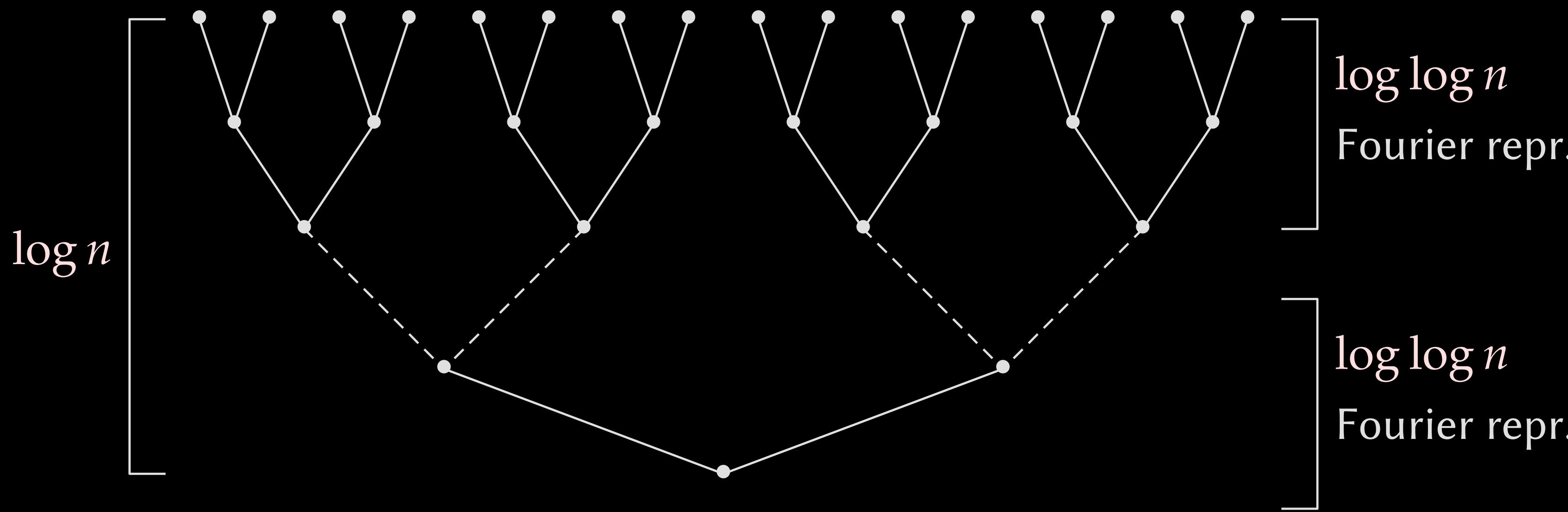
$\times 6$ $\quad \times\varepsilon^2$ $\quad \times 42$ $\quad \times\varepsilon^2$

$6+6\varepsilon+3\varepsilon^2+\varepsilon^3$ $\quad 210+42\varepsilon+7\varepsilon^2+\varepsilon^3$ $\quad \approx$32 bits

$\times 840$ $\quad \times\varepsilon^4$

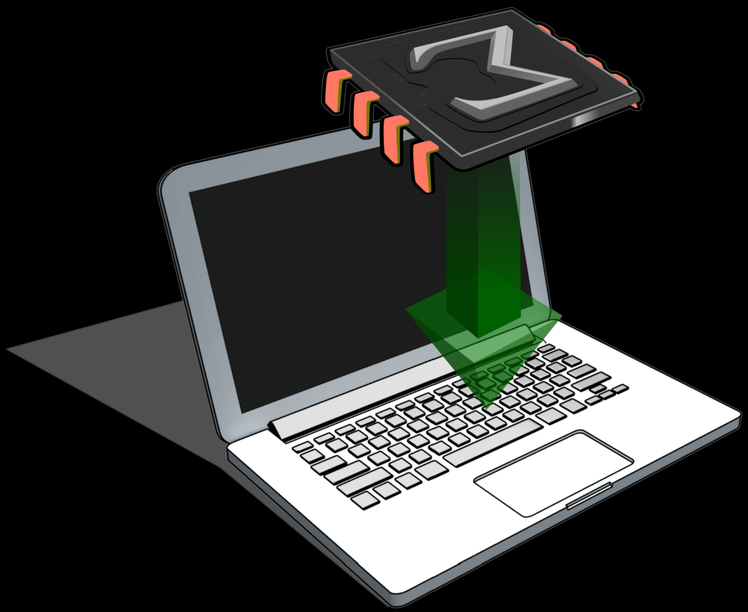
$5040+5040\varepsilon+2520\varepsilon^2+840\varepsilon^3+210\varepsilon^4+42\varepsilon^5+7\varepsilon^6+\varepsilon^7$ $\quad \approx$64 bits

FFT trading



Binary splitting exponentiation in time $O\left(\mathsf{M}(n)\,\frac{\log^2 n}{\log\log n}\right)$

Thank you !



http://www.texmacs.org