# Schoenhage-Strassen-Multiplication

**simplified, with slightly higher complexity**

# subdividing operands into blocks

- Inputs $u, v \in \mathbb{B}^N$ , $N = 2^k$ , $k \in \mathbb{N}$
- subdivide into $n$ blocks $u_i, v_i$ of block size $b$

$$b = 2^{\lfloor k/2 \rfloor} \leq \sqrt{N} \quad , \quad n = 2^{\lceil k/2 \rceil} < 2\sqrt{N}$$

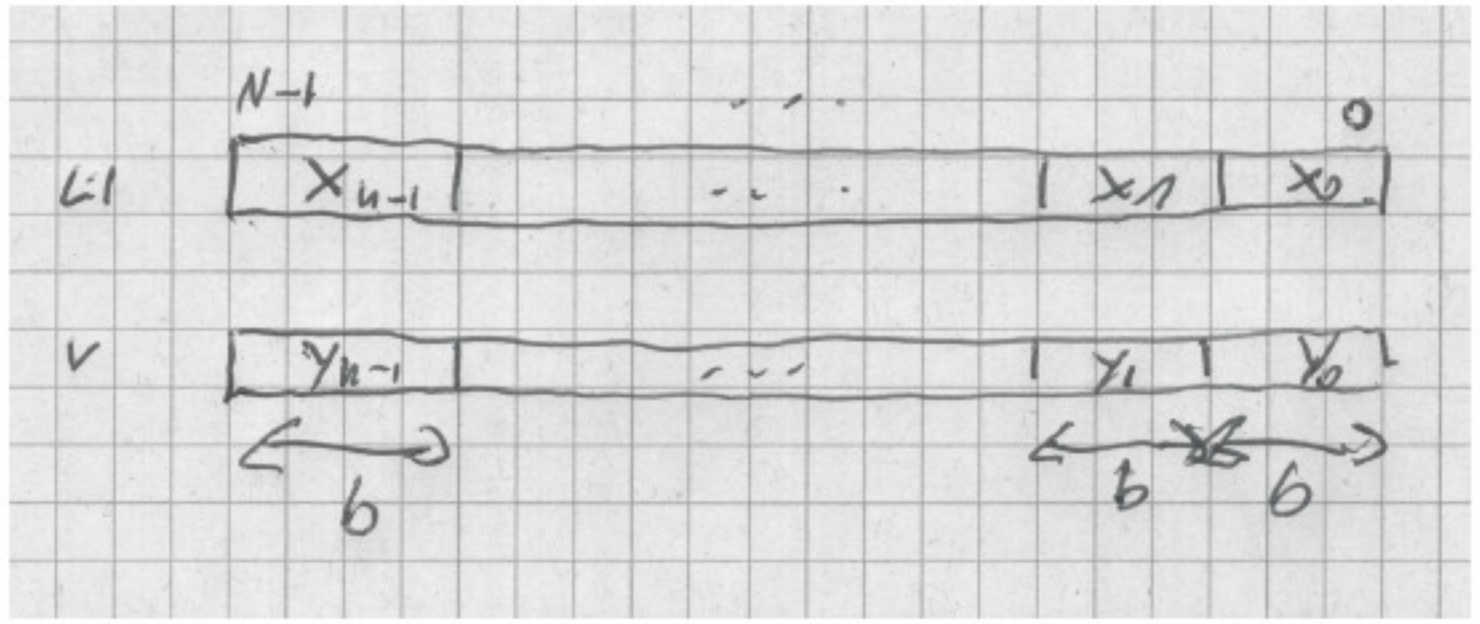

Figure 2: Subdividing operands into blocks of size $b$.

# subdividing operands into blocks

- Inputs $u, v \in \mathbb{B}^N$ , $N = 2^k$ , $k \in \mathbb{N}$
- subdivide into $n$ blocks $u_i, v_i$ of block size $b$

$$b = 2^{\lfloor k/2 \rfloor} \leq \sqrt{N} \quad , \quad n = 2^{\lceil k/2 \rceil} < 2\sqrt{N}$$

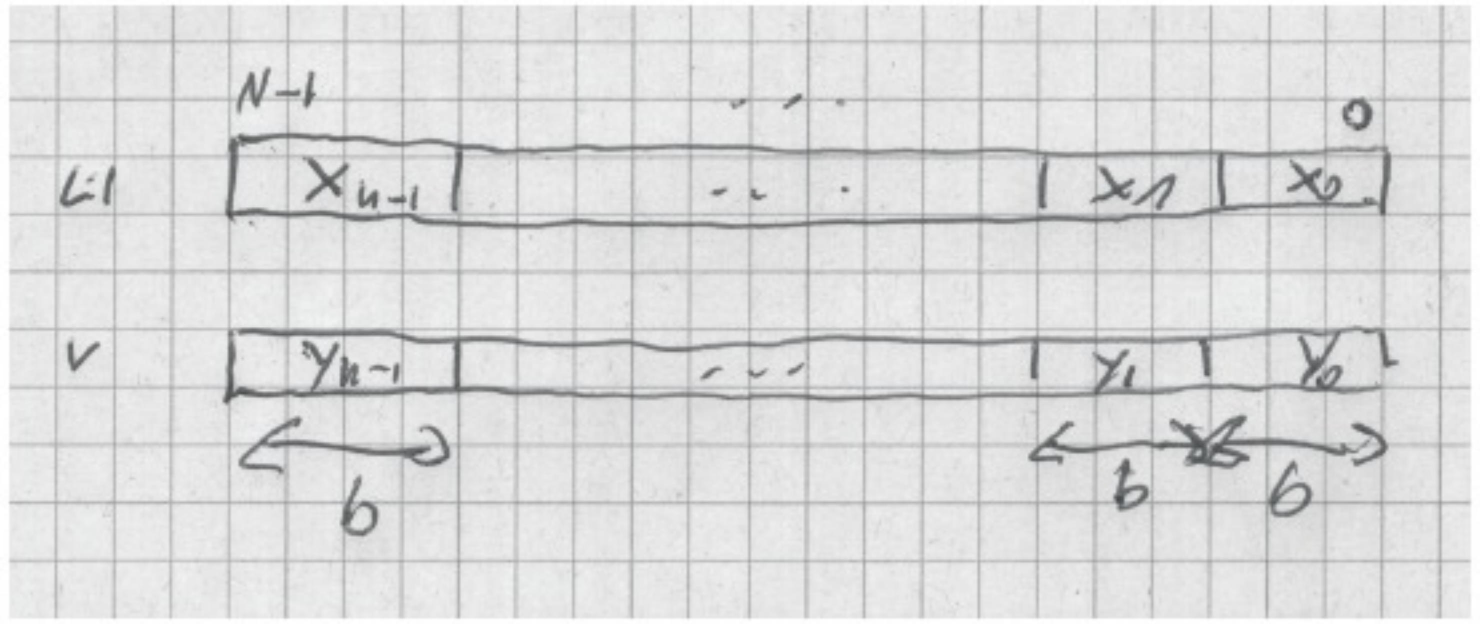


Figure 2: Subdividing operands into blocks of size $b$.

- name blocks $u_i, v_i \in \mathbb{B}^b$

$$\begin{aligned} u &= x_{n-1} \circ \ldots \circ x_0 \\ v &= y_{n-1} \circ \ldots \circ y_0 \end{aligned}$$

and their values

$$X_i = \langle x_i \rangle \quad , \quad Y_i = \langle y_i \rangle$$

Set

$$X_i = Y_i = 0 \quad \text{for} \quad i \geq n$$

# subdividing operands into blocks

- Inputs $u, v \in \mathbb{B}^N$ , $N = 2^k$ , $k \in \mathbb{N}$
- subdivide into $n$ blocks $u_i, v_i$ of block size $b$

$$b = 2^{\lfloor k/2 \rfloor} \leq \sqrt{N} \quad , \quad n = 2^{\lceil k/2 \rceil} < 2\sqrt{N}$$

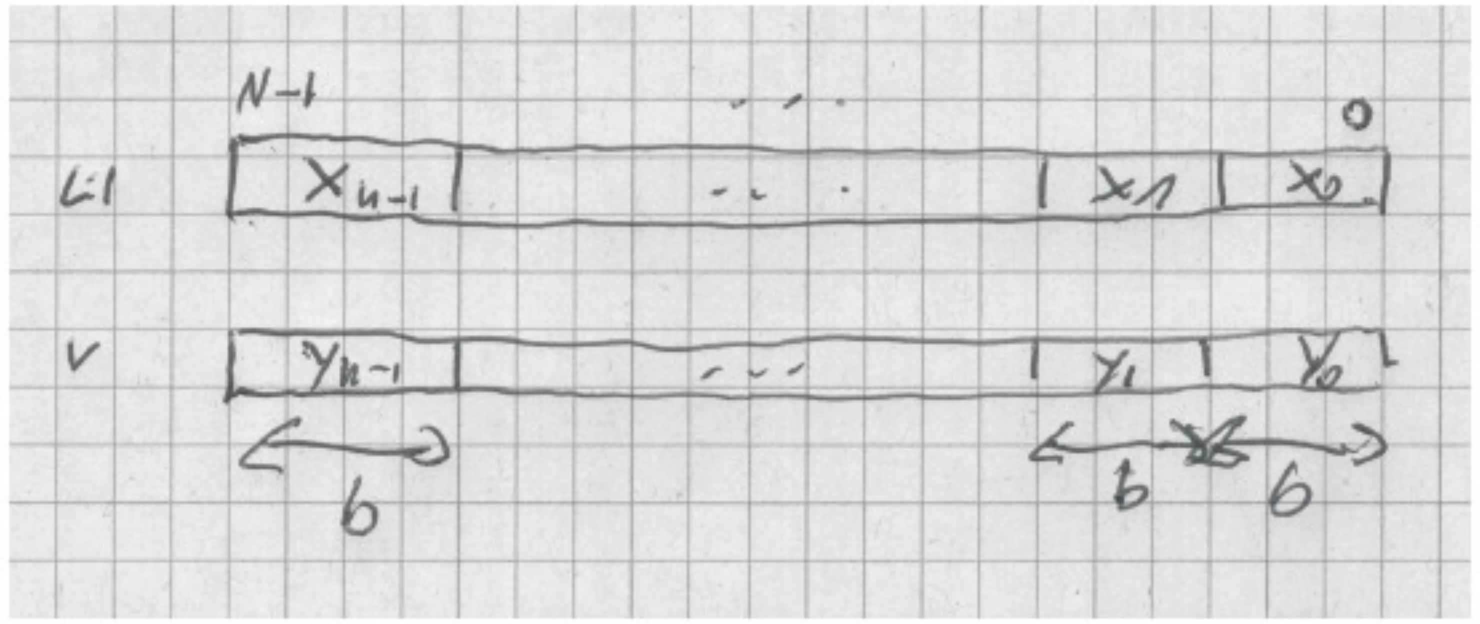

Figure 2: Subdividing operands into blocks of size $b$.

- name blocks $u_i, v_i \in \mathbb{B}^b$

$$\begin{aligned} u &= x_{n-1} \circ \ldots \circ x_0 \\ v &= y_{n-1} \circ \ldots \circ y_0 \end{aligned}$$

and their values

$$X_i = \langle x_i \rangle \quad , \quad Y_i = \langle y_i \rangle$$

Set

$$X_i = Y_i = 0 \quad \text{for} \quad i \geq n$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned} \langle u \rangle \cdot \langle v \rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1) \\ &= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2) \\ &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3) \end{aligned}$$

# subdividing operands into blocks

- Inputs $u, v \in \mathbb{B}^N$ , $N = 2^k$ , $k \in \mathbb{N}$
- subdivide into $n$ blocks $u_i, v_i$ of block size $b$

$$b = 2^{\lfloor k/2 \rfloor} \leq \sqrt{N} \quad , \quad n = 2^{\lceil k/2 \rceil} < 2\sqrt{N}$$

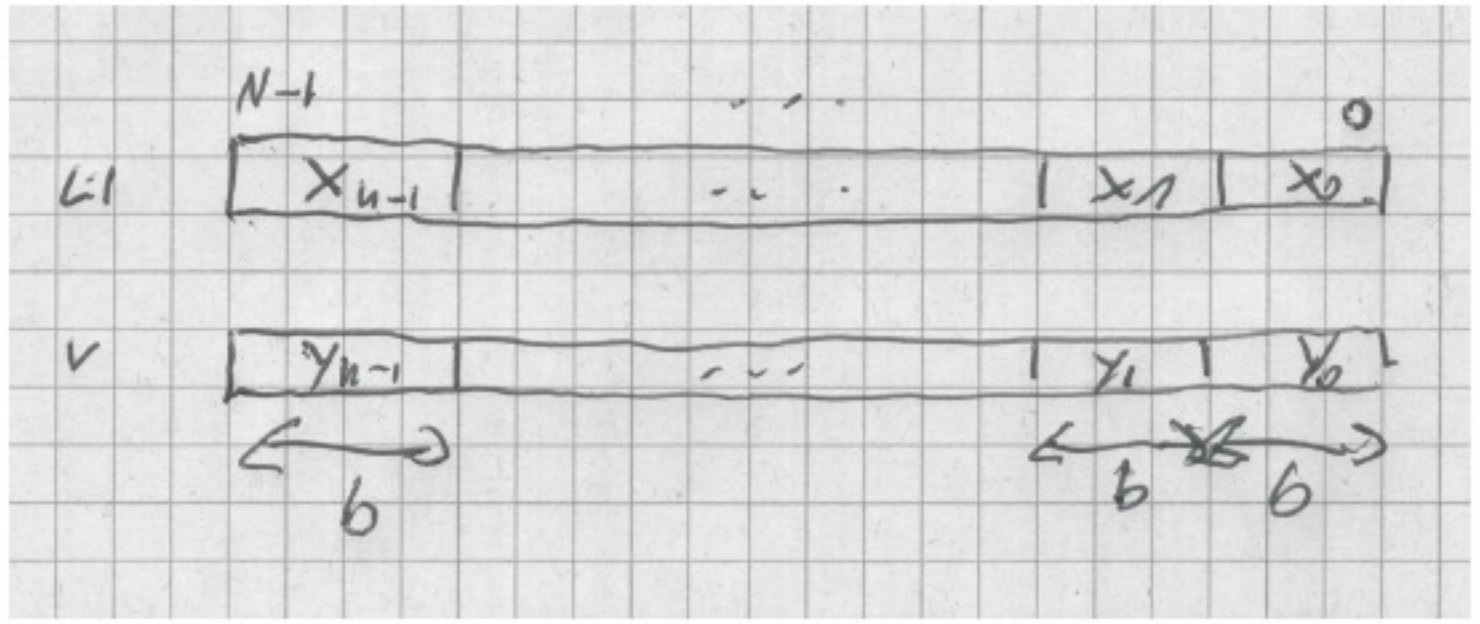


Figure 2: Subdividing operands into blocks of size $b$.

- name blocks $u_i, v_i \in \mathbb{B}^b$

$$\begin{aligned} u &= x_{n-1} \circ \ldots \circ x_0 \\ v &= y_{n-1} \circ \ldots \circ y_0 \end{aligned}$$

and their values

$$X_i = \langle x_i \rangle \quad , \quad Y_i = \langle y_i \rangle$$

Set

$$X_i = Y_i = 0 \quad \text{for} \quad i \geq n$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned} \langle u \rangle \cdot \langle v \rangle &= \left(\sum_{i=0}^{n-1} X_i \cdot 2^{bi}\right) \cdot \left(\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}\right) && (1) \\ &= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2) \\ &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3) \end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

No loss of precision if

$$(X \otimes Y)_i \leq 2^{2b} n < \omega^n + 1$$

# subdividing operands into blocks

- Inputs $u, v \in \mathbb{B}^N$ , $N = 2^k$ , $k \in \mathbb{N}$
- subdivide into $n$ blocks $u_i, v_i$ of block size $b$

$$b = 2^{\lfloor k/2 \rfloor} \leq \sqrt{N} \quad , \quad n = 2^{\lceil k/2 \rceil} < 2\sqrt{N}$$

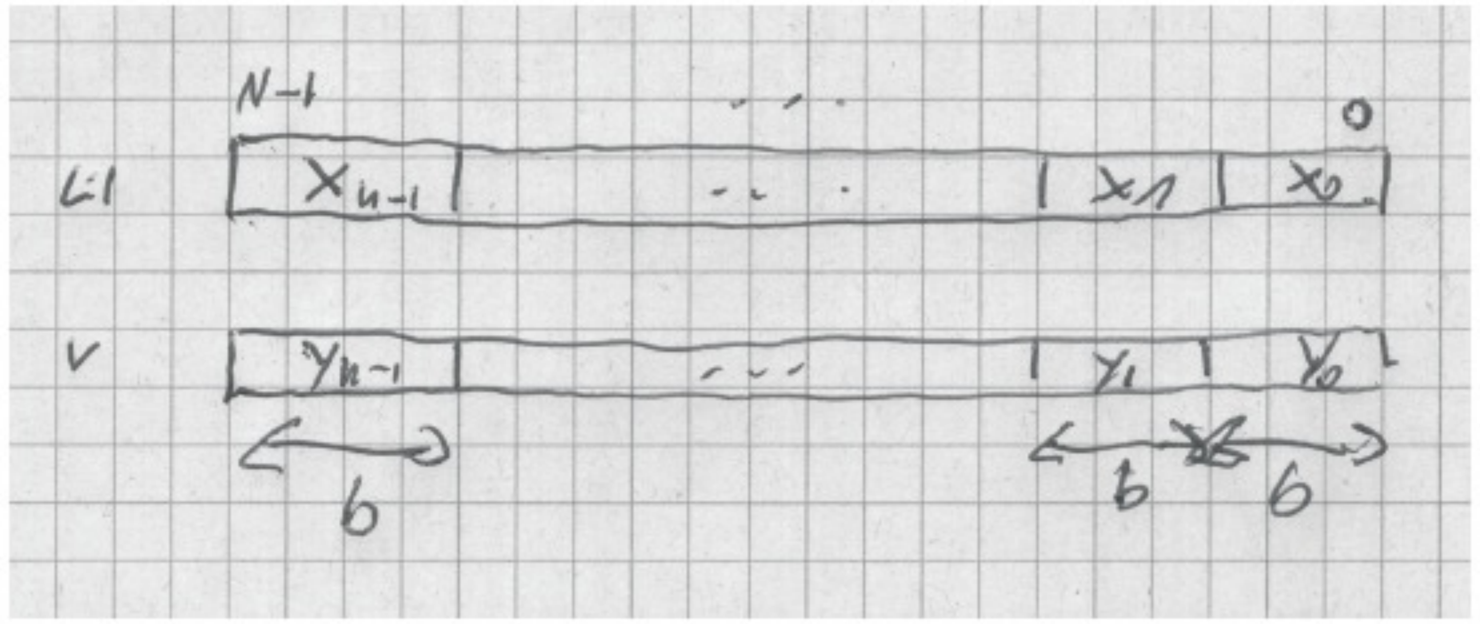


Figure 2: Subdividing operands into blocks of size $b$.

- name blocks $u_i, v_i \in \mathbb{B}^b$

$$\begin{aligned} u &= x_{n-1} \circ \ldots \circ x_0 \\ v &= y_{n-1} \circ \ldots \circ y_0 \end{aligned}$$

and their values

$$X_i = \langle x_i \rangle \quad , \quad Y_i = \langle y_i \rangle$$

Set

$$X_i = Y_i = 0 \quad \text{for} \quad i \geq n$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned} \langle u \rangle \cdot \langle v \rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1) \\ &= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2) \\ &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3) \end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

No loss of precision if

$$(X \otimes Y)_i \leq 2^{2b} n < \omega^n + 1$$

Sufficient

$$\begin{aligned} 2b + \log n &< n \log \omega \\ 2n + \log n &< n \log \omega \\ 3n &\leq n \log \omega \\ \omega &= 8 \end{aligned}$$

Thus

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$3n + 1$ bit arithmetic suffices for operations in $\mathbb{Z}_m$.

- Plan to compute the product of $u$ and $v$ as a convolution

$$
\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= \left(\sum_{i=0}^{n-1} X_i \cdot 2^{bi}\right) \cdot \left(\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}\right) && (1)\\
&= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}
$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$$\boxed{3n + 1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$$

# circuit complexity

- Plan to compute the product of $u$ and $v$ as a convolution

$$\langle u\rangle \cdot \langle v\rangle = (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) \quad (1)$$

$$= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} \quad (2)$$

$$= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} \quad (3)$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

– additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

– multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

## circuit complexity

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= \left(\sum_{i=0}^{n-1} X_i \cdot 2^{bi}\right) \cdot \left(\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}\right) && (1)\\
&= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$$

- additions and subtractions in FFT, IFFT: $O(2n\log(2n))$, each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

- modulo computations: for $Z \in [0 : 2^{3n+1} - 1]$ compute

$$Z \bmod M = Z \bmod \omega^n + 1$$

$$Z - (\omega^n + 1) \leq 2^{3n+1} - 1 - (2^{3n} + 1) = 2^{3n}$$

At most 1 subtraction needed.

$$Z \bmod \omega^n + 1 = \begin{cases} Z - (2^{3n} + 1) & Z - (2^{3n} + 1) > 0 \\ Z & \text{otherwise} \end{cases}$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle\cdot\langle v\rangle &= (\sum_{i=0}^{n-1} X_i\cdot 2^{bi})\cdot(\sum_{i=0}^{n-1} Y_i\cdot 2^{bi}) && (1)\\
&= \sum_{i=0}^{2n-1}\sum_{j=0}^{i} X_jY_{i-j}2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1}(X\otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X\otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m=\omega^n+1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X\otimes Y)_i < 2^{n\log\omega} = 2^{3n}$$

$3n+1$ bit arithmetic suffices for operations in $\mathbb{Z}_m$.

- additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2\cdot\log n)=O(N\cdot\log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n\cdot C(3n+1) < 4\sqrt{N}\cdot C(6\sqrt{N})$$

# circuit complexity

- modulo computations: for $Z\in[0:2^{3n+1}-1]$ compute

$$Z \bmod M = Z \bmod \omega^n+1$$

$$Z-(\omega^n+1)\le 2^{3n+1}-1-(2^{3n}+1)=2^{3n}$$

At most 1 subtraction needed.

$$Z \quad \bmod \omega^n+1 = \begin{cases} Z-(2^{3n}+1) & Z-(2^{3n}+1)>0\\ Z & \text{otherwise}\end{cases}$$

Cost $O(n)$. All $O(n\log n)$ ring operations (including multiplications)

$$O(n^2\log n)=O(N\log N)$$

## circuit complexity

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= \left(\sum_{i=0}^{n-1} X_i \cdot 2^{bi}\right)\cdot\left(\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}\right) && (1)\\
&= \sum_{i=0}^{2n-1}\sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X\otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X\otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X\otimes Y)_i < 2^{n\log\omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N}\cdot C(6\sqrt{N})$$

- modulo computations: $O(n^2 \log n) = O(N \log N)$

## circuit complexity

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1)\\
&= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2n log(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

- modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum.

$$\begin{aligned}
\langle z_i\rangle &= (X \otimes Y)_i\\
&\leq 2^{2b} n\\
&= 2^{2b+\log n}\\
&\leq 2^{2b+\log(2b)}\\
&= 2^{2b+\log b+1}\\
&\leq 2^{3b} \quad \text{for } b \geq 2\\
z_i &\in \mathbb{B}^{3b}
\end{aligned}$$

## circuit complexity

- Plan to compute the product of $u$ and $v$ as a convolution

$$\langle u\rangle \cdot \langle v\rangle = (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) \quad (1)$$
$$= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} \quad (2)$$
$$= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} \quad (3)$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

– additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

– multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

– modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum.

$$\begin{aligned}
\langle z_i\rangle &= (X \otimes Y)_i \\
&\le 2^{2b} n \\
&= 2^{2b+\log n} \\
&\le 2^{2b+\log(2b)} \\
&= 2^{2b+\log b+1} \\
&\le 2^{3b} \quad \text{for } b \ge 2 \\
z_i &\in \mathbb{B}^{3b}
\end{aligned}$$

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} \\
&= S_0 + S_1 + S_2 \\
S_x &= \sum_{i \equiv x \mod 3} (X \otimes Y)_i 2^{bi}
\end{aligned}$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}\langle u\rangle\cdot\langle v\rangle &= \left(\sum_{i=0}^{n-1} X_i\cdot 2^{bi}\right)\cdot\left(\sum_{i=0}^{n-1} Y_i\cdot 2^{bi}\right) &(1)\\ &= \sum_{i=0}^{2n-1}\sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} &(2)\\ &= \sum_{i=0}^{2n-1}(X\otimes Y)_i 2^{bi}\quad\text{(convolution theorem)} &(3)\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X\otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m=\omega^n+1 \quad\rightarrow\quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X\otimes Y)_i < 2^{n\log\omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2n\log(2n))$ , each of circuit cost $O(3n)$

$$O(n^2\cdot\log n)=O(N\cdot\log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n\cdot C(3n+1) < 4\sqrt{N}\cdot C(6\sqrt{N})$$

## circuit complexity

- modulo computations: $O(n^2\log n)=O(N\log N)$

- compute the final sum.

$$\begin{aligned}\langle z_i\rangle &= (X\otimes Y)_i\\ &\le 2^{2b}n\\ &= 2^{2b+\log n}\\ &\le 2^{2b+\log(2b)}\\ &= 2^{2b+\log b+1}\\ &\le 2^{3b}\quad \text{for } b\ge 2\\ z_i &\in \mathbb{B}^{3b}\end{aligned}$$

$$\begin{aligned}\langle u\rangle\cdot\langle v\rangle &= \sum_{i=0}^{2n-1}(X\otimes Y)_i 2^{bi}\quad\text{(convolution theorem)}\\ &= S_0+S_1+S_2\\ S_x &= \sum_{i\equiv x \mod 3}(X\otimes Y)_i 2^{bi}\end{aligned}$$

Compute each $S_x$ by concatenation

$$\begin{aligned}S_0 &= \langle \ldots\circ z_6\circ z_3\circ z_0\rangle\\ S_1 &= \langle \ldots\circ z_7\circ z_4\circ z_1\circ 0^b\rangle\\ S_2 &= \langle \ldots\circ z_8\circ z_5\circ z_2\circ 0^{2b}\rangle\end{aligned}$$

Add these 3 numbers of length $N+2b=O(n)$. Circuit cost $O(n)$.

- Plan to compute the product of $u$ and $v$ as a convolution

$$\langle u\rangle \cdot \langle v\rangle = (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) \tag{1}$$
$$= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} \tag{2}$$
$$= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} \tag{3}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

- modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum. Circuit cost $O(n)$.

## difference equation

Large $N$, some $A$:

$$\boxed{\begin{aligned} M(N) &\leq O(N \log N) + 4\sqrt{N} \cdot M(6\sqrt{N}) \\ &\leq AN \log N + 4\sqrt{N} \cdot M(6\sqrt{N}) \end{aligned}}$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1)\\
&= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2n log(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

## difference equation

- modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum. Circuit cost $O(n)$.

Large $N$, some $A$:

$$\boxed{\begin{aligned}
M(N) &\le O(N \log N) + 4\sqrt{N} \cdot M(6\sqrt{N})\\
&\le AN \log N + 4\sqrt{N} \cdot M(6\sqrt{N})
\end{aligned}}$$

$$\begin{aligned}
M'(N) &:= M(N)/N\\
M'(N) &\le A \log N + 4 \cdot 6 \cdot M'(6\sqrt{N})
\end{aligned}$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned} \langle u\rangle \cdot \langle v\rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1) \\ &= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2) \\ &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3) \end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

## difference equation

- modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum. Circuit cost $O(n)$.

Large $N$, some $A$:

$$\boxed{\begin{aligned} M(N) &\leq O(N \log N) + 4\sqrt{N} \cdot M(6\sqrt{N}) \\ &\leq AN \log N + 4\sqrt{N} \cdot M(6\sqrt{N}) \end{aligned}}$$

$$\begin{aligned} M'(N) &:= M(N)/N \\ M'(N) &\leq A \log N + 4 \cdot 6 \cdot M'(6\sqrt{N}) \end{aligned}$$

Guess

$$M'(N) \leq (B \log N)^x \quad \text{with} \quad B \geq A$$

Induction step

$$M'(N) \leq A \log N + 24B(\log(6\sqrt{N}))^x \leq B(\log N)^x$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}\langle u\rangle \cdot \langle v\rangle &= (\sum_{i=0}^{n-1} X_i \cdot 2^{bi}) \cdot (\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}) && (1)\\ &= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\ &= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$\boxed{3n+1 \text{ bit arithmetic suffices for operations in } \mathbb{Z}_m.}$

- additions and subtractions in FFT, IFFT: $O(2nlog(2n))$ , each of circuit cost $O(3n)$

$$O(n^2 \cdot \log n) = O(N \cdot \log N)$$

- multiplications: $2n$ for componentwise products of $3n+1$ bit numbers. Construct multiplier recursively. Let $C(N)$ = circuit cost of $N$ bit multiplier

$$2n \cdot C(3n+1) < 4\sqrt{N} \cdot C(6\sqrt{N})$$

## difference equation

- modulo computations: $O(n^2 \log n) = O(N \log N)$

- compute the final sum. Circuit cost $O(n)$.

Large $N$, some $A$:

$$\boxed{\begin{aligned} M(N) &\leq O(N \log N) + 4\sqrt{N} \cdot M(6\sqrt{N}) \\ &\leq AN \log N + 4\sqrt{N} \cdot M(6\sqrt{N}) \end{aligned}}$$

$$\begin{aligned} M'(N) &:= M(N)/N \\ M'(N) &\leq A \log N + 4 \cdot 6 \cdot M'(6\sqrt{N}) \end{aligned}$$

Guess

$$M'(N) \leq (B \log N)^x \quad \text{with} \quad B \geq A$$

Induction step

$$M'(N) \leq A \log N + 24B(\log(6\sqrt{N}))^x \leq B(\log N)^x$$

Sufficient:

$$\begin{aligned} \log N + 24(\log(6\sqrt{N}))^x &\leq (\log n)^x \quad (B \geq A) \\ \log N + 24(\log 6 + \frac{1}{2}\log N)^x &\leq (\log n)^x \\ 24(\frac{1}{2}\log N)^x + O(\log N)^{x-1}) &\leq (\log n)^x \\ \frac{24}{2^x}(\log N)^x + O(\log N)^{x-1} &\leq (\log n)^x \\ x &\geq 5 \end{aligned}$$

- Plan to compute the product of $u$ and $v$ as a convolution

$$\begin{aligned}
\langle u\rangle \cdot \langle v\rangle &= \Big(\sum_{i=0}^{n-1} X_i \cdot 2^{bi}\Big) \cdot \Big(\sum_{i=0}^{n-1} Y_i \cdot 2^{bi}\Big) && (1)\\
&= \sum_{i=0}^{2n-1} \sum_{j=0}^{i} X_j Y_{i-j} 2^{bi} && (2)\\
&= \sum_{i=0}^{2n-1} (X \otimes Y)_i 2^{bi} \quad \text{(convolution theorem)} && (3)
\end{aligned}$$

- choose $\omega$ and $n$ large enough such that coefficients $(X \otimes Y)_i$ of convolution can be computed in $\mathbb{Z}_m$ without loss of precision.

$$m = \omega^n + 1 \quad \rightarrow \quad \omega \text{ is } 2n\text{'th root of unity}$$

$$\omega = 8$$

$$(X \otimes Y)_i < 2^{n \log \omega} = 2^{3n}$$

$3n+1$ bit arithmetic suffices for operations in $\mathbb{Z}_m$.

Total cost

$$M(N) = O(N(\log N)^5)$$

Schoenhage Strassen with more involved construction

$$M(N) = O(N \log N \log\log N)$$

## difference equation

Large $N$, some $A$:

$$\begin{aligned}
M(N) &\le O(N \log N) + 4\sqrt{N} \cdot M(6\sqrt{N})\\
&\le AN \log N + 4\sqrt{N} \cdot M(6\sqrt{N})
\end{aligned}$$

$$\begin{aligned}
M'(N) &:= M(N)/N\\
M'(N) &\le A \log N + 4 \cdot 6 \cdot M'(6\sqrt{N})
\end{aligned}$$

Guess

$$M'(N) \le (B \log N)^x \quad \text{with} \quad B \ge A$$

Induction step

$$M'(N) \le A \log N + 24B(\log(6\sqrt{N}))^x \le B(\log N)^x$$

Sufficient:

$$\begin{aligned}
\log N + 24(\log(6\sqrt{N}))^x &\le (\log n)^x \quad (B \ge A)\\
\log N + 24(\log 6 + \frac{1}{2}\log N)^x &\le (\log n)^x\\
24(\frac{1}{2}\log N)^x + O(\log N)^{x-1}) &\le (\log n)^x\\
\frac{24}{2^x}(\log N)^x + O(\log N)^{x-1} &\le (\log n)^x\\
x &\ge 5
\end{aligned}$$