6.2 Master Theorem

Lemma 1

Let $a \ge 1, b \ge 1$ and $\epsilon > 0$ denote constants. Consider the recurrence

$$T(n) = aT\left(\frac{n}{b}\right) + f(n) .$$

Case 1.

If
$$f(n) = \mathcal{O}(n^{\log_b(a) - \epsilon})$$
 then $T(n) = \Theta(n^{\log_b a})$.

Case 2.

If
$$f(n) = \Theta(n^{\log_b(a)} \log^k n)$$
 then $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$, $k \ge 0$.

Case 3.

If
$$f(n) = \Omega(n^{\log_b(a) + \epsilon})$$
 and for sufficiently large n $af(\frac{n}{b}) \le cf(n)$ for some constant $c < 1$ then $T(n) = \Theta(f(n))$.



6.2 Master Theorem

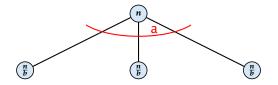
We prove the Master Theorem for the case that n is of the form b^{ℓ} , and we assume that the non-recursive case occurs for problem size 1 and incurs cost 1.



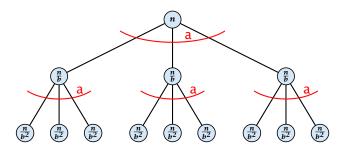




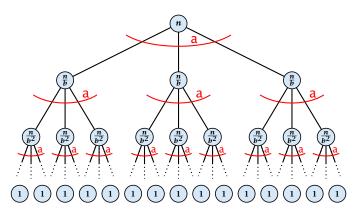






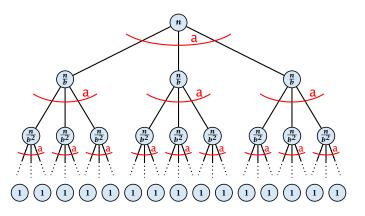






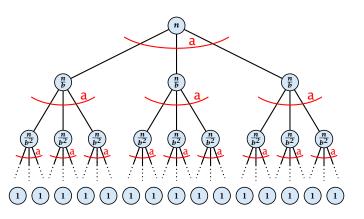


The running time of a recursive algorithm can be visualized by a recursion tree:



f(n)

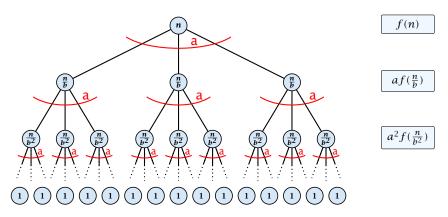
The running time of a recursive algorithm can be visualized by a recursion tree:



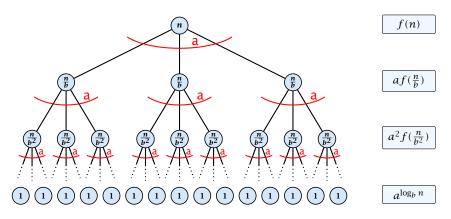
f(n)

 $af(\frac{n}{b})$

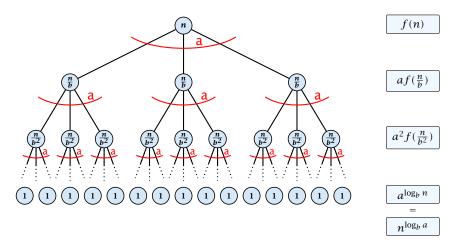












6.2 Master Theorem

This gives

$$T(n) = n^{\log_b a} + \sum_{i=0}^{\log_b n-1} a^i f\left(\frac{n}{b^i}\right) .$$



$$T(n) - n^{\log_b a}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$b^{-i(\log_b a - \epsilon)} = b^{\epsilon i} (b^{\log_b a})^{-i} = b^{\epsilon i} a^{-i}$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$b^{-i(\log_b a - \epsilon)} = b^{\epsilon i} (b^{\log_b a})^{-i} = b^{\epsilon i} a^{-i} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b a - \epsilon} (b^{\epsilon})^i$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$\underline{b^{-i(\log_b a - \epsilon)} = b^{\epsilon i}(b^{\log_b a})^{-i} = b^{\epsilon i}a^{-i}} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} \left(b^{\epsilon}\right)^i$$

$$\sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{q-1}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$\underline{b^{-i(\log_b a - \epsilon)} = b^{\epsilon i}(b^{\log_b a})^{-i} = b^{\epsilon i}a^{-i}} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} (b^{\epsilon})^i$$

$$\sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{a^{-1}} = c n^{\log_b a - \epsilon} (b^{\epsilon \log_b n} - 1)/(b^{\epsilon} - 1)$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$\underline{b^{-i(\log_b a - \epsilon)} = b^{\epsilon i}(b^{\log_b a})^{-i} = b^{\epsilon i}a^{-i}} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} (b^{\epsilon})^i$$

$$\underline{\sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{q - 1}} = c n^{\log_b a - \epsilon} (b^{\epsilon \log_b n} - 1) / (b^{\epsilon} - 1)$$

$$= c n^{\log_b a - \epsilon} (n^{\epsilon} - 1) / (b^{\epsilon} - 1)$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$\underline{b^{-i(\log_b a - \epsilon)} = b^{\epsilon i}(b^{\log_b a})^{-i} = b^{\epsilon i}a^{-i}} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} (b^{\epsilon})^i$$

$$\sum_{i=0}^k a^i = \frac{q^{k+1} - 1}{q - 1} = c n^{\log_b a - \epsilon} (b^{\epsilon \log_b n} - 1)/(b^{\epsilon} - 1)$$

$$= c n^{\log_b a - \epsilon} (n^{\epsilon} - 1)/(b^{\epsilon} - 1)$$

$$= \frac{c}{b^{\epsilon} - 1} n^{\log_b a} (n^{\epsilon} - 1)/(n^{\epsilon})$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$\underline{b^{-i(\log_b a - \epsilon)} = b^{\epsilon i}(b^{\log_b a})^{-i} = b^{\epsilon i}a^{-i}} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} (b^{\epsilon})^i$$

$$\underline{\sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{q - 1}} = c n^{\log_b a - \epsilon} (b^{\epsilon \log_b n} - 1)/(b^{\epsilon} - 1)$$

$$= c n^{\log_b a - \epsilon} (n^{\epsilon} - 1)/(b^{\epsilon} - 1)$$

$$= \frac{c}{b^{\epsilon} - 1} n^{\log_b a} (n^{\epsilon} - 1)/(n^{\epsilon})$$

Hence,

$$T(n) \le \left(\frac{c}{h^{\epsilon} - 1} + 1\right) n^{\log_b(a)}$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a - \epsilon}$$

$$b^{-i(\log_b a - \epsilon)} = b^{\epsilon i} (b^{\log_b a})^{-i} = b^{\epsilon i} a^{-i} = c n^{\log_b a - \epsilon} \sum_{i=0}^{\log_b n - 1} (b^{\epsilon})^i$$

$$\sum_{i=0}^{k} q^{i} = \frac{q^{k+1}-1}{q-1} = c n^{\log_b a - \epsilon} (b^{\epsilon \log_b n} - 1)/(b^{\epsilon} - 1)$$

$$= c n^{\log_b a - \epsilon} (n^{\epsilon} - 1)/(b^{\epsilon} - 1)$$

$$= \frac{c}{b\epsilon - 1} n^{\log_b a} (n^{\epsilon} - 1)/(n^{\epsilon})$$

Hence,

$$T(n) \le \left(\frac{c}{h^{\epsilon} - 1} + 1\right) n^{\log_b(a)}$$

$$\Rightarrow T(n) = \mathcal{O}(n^{\log_b a}).$$



$$T(n) - n^{\log_b a}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

Hence,

$$T(n) = \mathcal{O}(n^{\log_b a} \log_b n)$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

Hence,

$$T(n) = \mathcal{O}(n^{\log_b a} \log_b n)$$

$$T(n) = \mathcal{O}(n^{\log_b a} \log_b n)$$
 $\Rightarrow T(n) = \mathcal{O}(n^{\log_b a} \log n).$



$$T(n) - n^{\log_b a}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$



$$\begin{split} T(n) - n^{\log_b a} &= \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right) \\ &\geq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \end{split}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\geq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\geq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\geq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

Hence,

$$T(n) = \mathbf{\Omega}(n^{\log_b a} \log_b n)$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\geq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a}$$

$$= c n^{\log_b a} \sum_{i=0}^{\log_b n - 1} 1$$

$$= c n^{\log_b a} \log_b n$$

Hence,

$$T(n) = \mathbf{\Omega}(n^{\log_b a} \log_b n)$$
 $\Rightarrow T(n) = \mathbf{\Omega}(n^{\log_b a} \log n).$



$$T(n) - n^{\log_b a}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$n=b^\ell\Rightarrow \ell=\log_b n$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$\boxed{n = b^\ell \Rightarrow \ell = \log_b n} = c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^\ell}{b^i}\right)\right)^k$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$\boxed{n = b^{\ell} \Rightarrow \ell = \log_b n} = c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^{\ell}}{b^i}\right)\right)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} (\ell - i)^k$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$\boxed{n = b^\ell \Rightarrow \ell = \log_b n} = c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^\ell}{b^i}\right)\right)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} (\ell - i)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell} i^k$$



$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$\boxed{n = b^{\ell} \Rightarrow \ell = \log_b n} = c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^{\ell}}{b^i}\right)\right)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} (\ell - i)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell} i^k \geq \frac{1}{k} \ell^{k+1}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$\boxed{n = b^{\ell} \Rightarrow \ell = \log_b n} = c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^{\ell}}{b^i}\right)\right)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} (\ell - i)^k$$

$$= c n^{\log_b a} \sum_{i=1}^{\ell} i^k$$

$$\approx \frac{c}{b} n^{\log_b a} \ell^{k+1}$$

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq c \sum_{i=0}^{\log_b n - 1} a^i \left(\frac{n}{b^i}\right)^{\log_b a} \cdot \left(\log_b \left(\frac{n}{b^i}\right)\right)^k$$

$$n = b^{\ell} \Rightarrow \ell = \log_b n$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} \left(\log_b \left(\frac{b^{\ell}}{b^i}\right)\right)^k$$

$$= c n^{\log_b a} \sum_{i=0}^{\ell - 1} (\ell - i)^k$$

$$= c n^{\log_b a} \sum_{i=1}^{\ell} i^k$$

$$\approx \frac{c}{b} n^{\log_b a} \ell^{k+1} \qquad \Rightarrow T(n) = \mathcal{O}(n^{\log_b a} \log^{k+1} n).$$





From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.



From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$



From this we get $a^if(n/b^i) \le c^if(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq \sum_{i=0}^{\log_b n - 1} c^i f(n) + \mathcal{O}(n^{\log_b a})$$



From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq \sum_{i=0}^{\log_b n - 1} c^i f(n) + \mathcal{O}(n^{\log_b a})$$

$$q < 1: \sum_{i=0}^{n} q^{i} = \frac{1 - q^{n+1}}{1 - q} \le \frac{1}{1 - q}$$



From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq \sum_{i=0}^{\log_b n - 1} c^i f(n) + \mathcal{O}(n^{\log_b a})$$

$$q < 1: \sum_{i=0}^n q^i = \frac{1 - q^{n+1}}{1 - q} \leq \frac{1}{1 - c} f(n) + \mathcal{O}(n^{\log_b a})$$



From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq \sum_{i=0}^{\log_b n - 1} c^i f(n) + \mathcal{O}(n^{\log_b a})$$

$$q < 1: \sum_{i=0}^n q^i = \frac{1 - q^{n+1}}{1 - q} \leq \frac{1}{1 - c} f(n) + \mathcal{O}(n^{\log_b a})$$

Hence,

$$T(n) \le \mathcal{O}(f(n))$$



From this we get $a^i f(n/b^i) \le c^i f(n)$, where we assume that $n/b^{i-1} \ge n_0$ is still sufficiently large.

$$T(n) - n^{\log_b a} = \sum_{i=0}^{\log_b n - 1} a^i f\left(\frac{n}{b^i}\right)$$

$$\leq \sum_{i=0}^{\log_b n - 1} c^i f(n) + \mathcal{O}(n^{\log_b a})$$

$$q < 1: \sum_{i=0}^n q^i = \frac{1 - q^{n+1}}{1 - q} \leq \frac{1}{1 - c} f(n) + \mathcal{O}(n^{\log_b a})$$

Hence,

$$T(n) \leq \mathcal{O}(f(n))$$

$$\Rightarrow T(n) = \Theta(f(n)).$$



Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



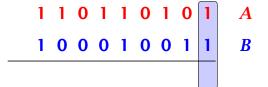
Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.

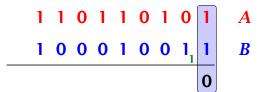


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



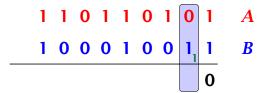


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



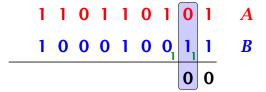


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



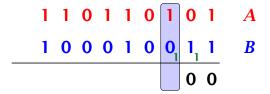


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



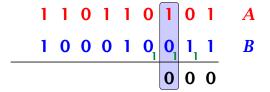


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



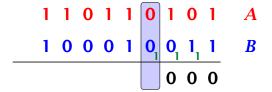


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



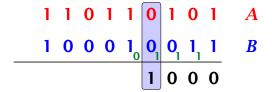


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



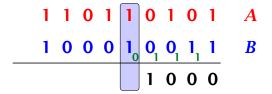


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



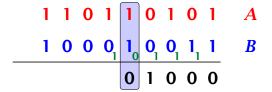


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



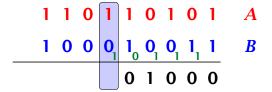


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



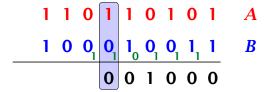


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



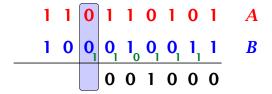


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



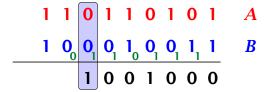


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



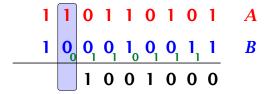


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



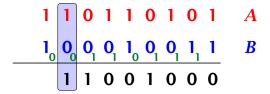


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



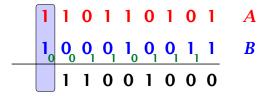


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



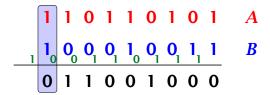


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



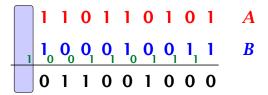


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.



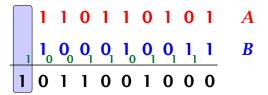


Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.





Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.





Suppose we want to multiply two n-bit Integers, but our registers can only perform operations on integers of constant size.

For this we first need to be able to add two integers A and B:

This gives that two n-bit integers can be added in time $\mathcal{O}(n)$.





Suppose that we want to multiply an n-bit integer A and an m-bit integer B ($m \le n$).

1 0 0 0 1 × 1 0 1 1



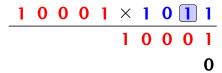
Suppose that we want to multiply an n-bit integer A and an m-bit integer B ($m \le n$).

1 0 0 0 1 × 1 0 1 1









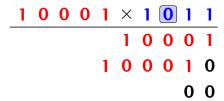












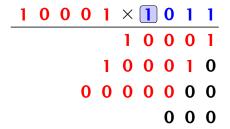


_	1	0	0	0	1	X	1	0	1	1
						1	0	0	0	1
					1	0	0	0	1	0
				0	0	0	0	0	0	0



_1	0	0	0	1	X	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0







1	0	0	0	1	X	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0
		1	0	0	0	1	0	0	0



1	0	0	0	1	X	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0
		1	0	0	0	1	0	0	0



_1	0	0	0	1	X	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0
		1	0	0	0	1	0	0	0
		1	0	1	1	1	0	1	1



Suppose that we want to multiply an n-bit integer A and an m-bit integer B ($m \le n$).

1	0	0	0	1	×	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0
		1	0	0	0	1	0	0	0
		1	0	1	1	1	0	1	1

Time requirement:



Suppose that we want to multiply an n-bit integer A and an m-bit integer B ($m \le n$).

1	0	0	0	1	×	1	0	1	1
					1	0	0	0	1
				1	0	0	0	1	0
			0	0	0	0	0	0	0
		1	0	0	0	1	0	0	0
		1	0	1	1	1	0	1	1

Time requirement:

▶ Computing intermediate results: O(nm).



Suppose that we want to multiply an n-bit integer A and an m-bit integer B ($m \le n$).

Time requirement:

- ▶ Computing intermediate results: O(nm).
- ► Adding m numbers of length $\leq 2n$: $\mathcal{O}((m+n)m) = \mathcal{O}(nm)$.



A recursive approach:

Suppose that integers \boldsymbol{A} and \boldsymbol{B} are of length $n=2^k$, for some k.



A recursive approach:

Suppose that integers \boldsymbol{A} and \boldsymbol{B} are of length $n=2^k$, for some k.





A recursive approach:

Suppose that integers **A** and **B** are of length $n = 2^k$, for some k.

 $\begin{bmatrix} b_n & \cdots & b_0 \end{bmatrix} \times \begin{bmatrix} a_n & \cdots & a_0 \end{bmatrix}$



A recursive approach:

Suppose that integers **A** and **B** are of length $n = 2^k$, for some k.

$$b_n \cdots b_{\frac{n}{2}} b_{\frac{n}{2}-1} \cdots b_0 \times a_n \cdots a_{\frac{n}{2}} a_{\frac{n}{2}-1} \cdots a_0$$



A recursive approach:

Suppose that integers \boldsymbol{A} and \boldsymbol{B} are of length $n=2^k$, for some k.

B_1	B ₀	×	A_1	A_0
-------	-----------------------	---	-------	-------

A recursive approach:

Suppose that integers **A** and **B** are of length $n = 2^k$, for some k.



Then it holds that

$$A = A_1 \cdot 2^{\frac{n}{2}} + A_0$$
 and $B = B_1 \cdot 2^{\frac{n}{2}} + B_0$



A recursive approach:

Suppose that integers **A** and **B** are of length $n = 2^k$, for some k.



Then it holds that

$$A = A_1 \cdot 2^{\frac{n}{2}} + A_0$$
 and $B = B_1 \cdot 2^{\frac{n}{2}} + B_0$

Hence,

$$A \cdot B = A_1 B_1 \cdot 2^n + (A_1 B_0 + A_0 B_1) \cdot 2^{\frac{n}{2}} + A_0 \cdot B_0$$



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)



Algorithm 3 mult(A, B)

Algorithm 3 mult(A, B)

Algorithm 3 mult(A, B)

1: if |A| = |B| = 1 then

2: return $a_0 \cdot b_0$ 3: split A into A_0 and A_1 4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_1 \leftarrow \text{mult}(A_1, B_0) + \text{mult}(A_0, B_1)$ 7: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 8: return $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$ O(1) O(n) O(

$$\mathcal{O}(1)$$

Algorithm 3 mult(A, B)

Algorithm 3 $mult(A, B)$	
1: if $ A = B = 1$ then	$\mathcal{O}(1)$
2: return $a_0 \cdot b_0$	$\mathcal{O}(1)$
3: $splitA$ into A_0 and A_1	$\mathcal{O}(n)$
4: split B into B_0 and B_1	$\mathcal{O}(n)$
$5: Z_2 \leftarrow \operatorname{mult}(A_1, B_1)$	$T(\frac{n}{2})$
6: $Z_1 \leftarrow \operatorname{mult}(A_1, B_0) + \operatorname{mult}(A_0, B_1)$	$2T(\frac{n}{2}) + \mathcal{O}(n)$
7: $Z_0 \leftarrow \operatorname{mult}(A_0, B_0)$	$T(\frac{n}{2})$
8: return $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$	$\mathcal{O}(n)$

We get the following recurrence:

$$T(n) = 4T\left(\frac{n}{2}\right) + \mathcal{O}(n) .$$



Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = O(n^{\log_b a \epsilon})$ $T(n) = O(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$



Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = O(n^{\log_b a \epsilon})$ $T(n) = O(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$

In our case a=4, b=2, and $f(n)=\Theta(n)$. Hence, we are in Case 1, since $n=\mathcal{O}(n^{2-\epsilon})=\mathcal{O}(n^{\log_b a-\epsilon})$.



Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = O(n^{\log_b a \epsilon})$ $T(n) = O(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- ► Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$

In our case a=4, b=2, and $f(n)=\Theta(n)$. Hence, we are in Case 1, since $n=\mathcal{O}(n^{2-\epsilon})=\mathcal{O}(n^{\log_b a-\epsilon})$.

We get a running time of $\mathcal{O}(n^2)$ for our algorithm.



Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = O(n^{\log_b a \epsilon})$ $T(n) = O(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$

In our case a=4, b=2, and $f(n)=\Theta(n)$. Hence, we are in Case 1, since $n=\mathcal{O}(n^{2-\epsilon})=\mathcal{O}(n^{\log_b a-\epsilon})$.

We get a running time of $\mathcal{O}(n^2)$ for our algorithm.

⇒ Not better then the "school method".





$$Z_1 = A_1 B_0 + A_0 B_1$$



$$Z_1 = A_1 B_0 + A_0 B_1$$

= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$



$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$



We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,



We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then**

2: return $a_0 \cdot b_0$

3: split A into A_0 and A_1

4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$



We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

3: split A into A_0 and A_1

4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$



We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

3: split A into A_0 and A_1

4: split A into A_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$

We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

3: split A into A_0 and A_1

4: split A into A_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$

$$\mathcal{O}(1)$$

$$\mathcal{O}(1)$$

$$\mathcal{O}(n)$$

We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

3: split A into A_0 and A_1

3: Split A little A_0 and B_1 4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$

$$\mathcal{O}(1)$$

$$\mathcal{O}(1)$$

$$\mathcal{O}(n)$$

$$\mathcal{O}(n)$$

We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

3: split A into A_0 and A_1

3: Split A into A_0 and B_1 4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$

$$\mathcal{O}(1)$$

$$\mathcal{O}(1)$$

$$\mathcal{O}(n)$$

$$\mathcal{O}(n)$$

$$T(\frac{n}{2})$$

We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = $Z_2 = Z_0$
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 mult(A, B)

1: **if** |A| = |B| = 1 **then** 2: **return** $a_0 \cdot b_0$

2: **return** $a_0 \cdot b_0$ 3: split A into A_0 and A_1 4: split B into B_0 and B_1 5: $Z_2 \leftarrow \text{mult}(A_1, B_1)$ 6: $Z_0 \leftarrow \text{mult}(A_0, B_0)$ 7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$ 8: **return** $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$

$$\mathcal{O}(1)$$

$$\mathcal{O}(1)$$

$$\mathcal{O}(n)$$

$$\mathcal{O}(n)$$

$$T(\frac{n}{2})$$

$$T(\frac{n}{2})$$

We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1$$
 = Z_2 = Z_0
= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,



We can use the following identity to compute Z_1 :

$$Z_1 = A_1 B_0 + A_0 B_1 = Z_2 = Z_0$$

= $(A_0 + A_1) \cdot (B_0 + B_1) - A_1 B_1 - A_0 B_0$

Hence,

Algorithm 4 $mult(A, B)$	
1: if $ A = B = 1$ then	$\mathcal{O}(1)$
2: return $a_0 \cdot b_0$	$\mathcal{O}(1)$
3: $splitA$ into A_0 and A_1	$\mathcal{O}(n)$
4: split B into B_0 and B_1	$\mathcal{O}(n)$
5: $Z_2 \leftarrow \operatorname{mult}(A_1, B_1)$	$T(\frac{n}{2})$
6: $Z_0 \leftarrow \operatorname{mult}(A_0, B_0)$	$T(\frac{n}{2})$
7: $Z_1 \leftarrow \text{mult}(A_0 + A_1, B_0 + B_1) - Z_2 - Z_0$	$T(\frac{n}{2}) + \mathcal{O}(n)$
8: return $Z_2 \cdot 2^n + Z_1 \cdot 2^{\frac{n}{2}} + Z_0$	$\mathcal{O}(n)$



We get the following recurrence:

$$T(n) = 3T\left(\frac{n}{2}\right) + \mathcal{O}(n) .$$

Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

Case 1:
$$f(n) = \mathcal{O}(n^{\log_b a - \epsilon})$$
 $T(n) = \Theta(n^{\log_b a})$

► Case 2:
$$f(n) = \Theta(n^{\log_b a} \log^k n)$$
 $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$

► Case 3:
$$f(n) = \Omega(n^{\log_b a + \epsilon})$$
 $T(n) = \Theta(f(n))$

Again we are in Case 1. We get a running time of $\Theta(n^{\log_2 3}) \approx \Theta(n^{1.59})$.





We get the following recurrence:

$$T(n) = 3T\left(\frac{n}{2}\right) + \mathcal{O}(n) .$$

Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

► Case 1:
$$f(n) = \mathcal{O}(n^{\log_b a - \epsilon})$$
 $T(n) = \Theta(n^{\log_b a})$

► Case 2:
$$f(n) = \Theta(n^{\log_b a} \log^k n)$$
 $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$

• Case 3:
$$f(n) = \Omega(n^{\log_b a + \epsilon})$$
 $T(n) = \Theta(f(n))$

Again we are in Case 1. We get a running time of $\Theta(n^{\log_2 3}) \approx \Theta(n^{1.59})$.





We get the following recurrence:

$$T(n) = 3T\left(\frac{n}{2}\right) + \mathcal{O}(n) .$$

Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = \mathcal{O}(n^{\log_b a \epsilon})$ $T(n) = \Theta(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$

Again we are in Case 1. We get a running time of $\Theta(n^{\log_2 3}) \approx \Theta(n^{1.59})$.



We get the following recurrence:

$$T(n) = 3T\left(\frac{n}{2}\right) + \mathcal{O}(n) .$$

Master Theorem: Recurrence: $T[n] = aT(\frac{n}{b}) + f(n)$.

- ► Case 1: $f(n) = \mathcal{O}(n^{\log_b a \epsilon})$ $T(n) = \Theta(n^{\log_b a})$
- ► Case 2: $f(n) = \Theta(n^{\log_b a} \log^k n)$ $T(n) = \Theta(n^{\log_b a} \log^{k+1} n)$
- Case 3: $f(n) = \Omega(n^{\log_b a + \epsilon})$ $T(n) = \Theta(f(n))$

Again we are in Case 1. We get a running time of $\Theta(n^{\log_2 3}) \approx \Theta(n^{1.59})$.

