

Integer multiplication and the Fast Fourier Transform

Multiplying n-bit integers

Karatsuba 1960

Input: $x, y \in \{0,1\}^n$

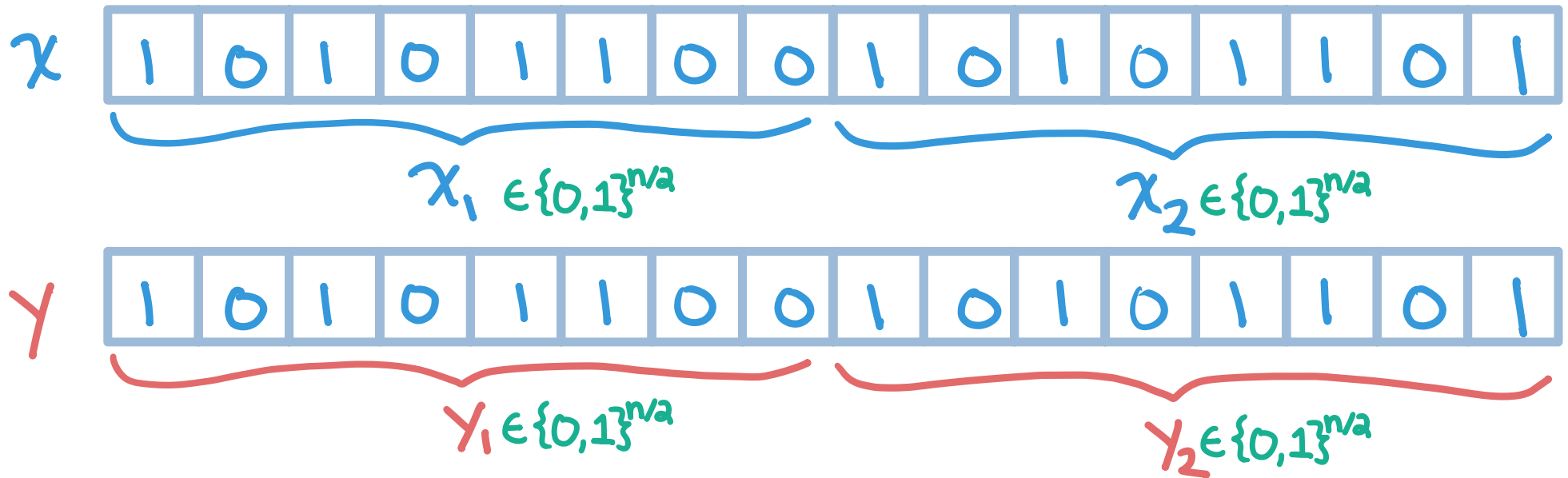
Output: product $(xy) \in \{0,1\}^{2n}$

$$\begin{array}{r} 1234 \\ \times 5678 \\ \hline 9872 \\ 8638 \\ + \\ \hline \end{array}$$

$O(n^2)$ time

Better?

Divide bits in half



$$x = x_1 2^{n/2} + x_2, \quad y = y_1 2^{n/2} + y_2$$

$$x \cdot y = \underbrace{x_1 y_1}_{\text{blue}} 2^n + \underbrace{(x_1 y_2 + y_1 x_2)}_{\text{blue}} 2^{n/2} + \underbrace{x_2 y_2}_{\text{blue}}$$

which multiplies 4 pairs of $(n/2)$ -bit numbers

$$x \cdot y = x_1 y_1 2^n + (x_1 y_2 + y_1 x_2) 2^{n/2} + x_2 y_2$$

Karatsuba's Trick

$$(x_1 + x_2)(y_1 + y_2) = x_1 y_1 + \underbrace{x_1 y_2 + x_2 y_1}_{\text{middle term}} + x_2 y_2$$

already computed

one multiply

$$x_1 y_2 + x_2 y_1 = (x_1 + x_2)(y_1 + y_2) - x_1 y_1 - x_2 y_2$$

2 multiplies for the price of 1 (more)!

① Recursive specification

Designing a recursive algorithm

① Recursive specification

- declares input/output of algo
- "contract" algo must fulfill
- induction hypothesis for correctness

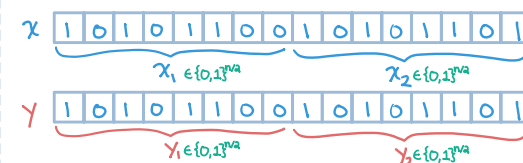
② Implement spec

③ Prove correctness

argue algo satisfies recursive
for all n by induction on n spec

$\text{multiply}(x[1..n], y[1..n]) = \text{the } (2n\text{-bit integer}) \text{ product of } x \text{ and } y$
(as n -bit integers).

Divide bits in half



$$x = x_1 2^{n/2} + x_2, \quad y = y_1 2^{n/2} + y_2$$

$$x \cdot y = \underbrace{x_1 y_1}_{\text{one multiply}} 2^n + \underbrace{(x_1 y_2 + y_1 x_2)}_{\text{middle term}} 2^{n/2} + \underbrace{x_2 y_2}_{\text{one multiply}}$$

which multiplies 4 pairs of $(n/2)$ -bit numbers

Karatsuba's Trick

$$\underbrace{(x_1 + x_2)(y_1 + y_2)}_{\text{one multiply}} = x_1 y_1 + \underbrace{x_1 y_2 + x_2 y_1}_{\text{middle term}} + x_2 y_2$$

already computed

$$x_1 y_2 + x_2 y_1 = x_1 y_1 + x_2 y_2 - (x_1 + x_2)(y_1 + y_2)$$

2 multiplies for the price of 1 (more)!

Designing a recursive algorithm

① Recursive specification

- declares input/output of algo
- "contract" algo must fulfill
- induction hypothesis for correctness

② Implement spec

③ Prove correctness

argue algo satisfies recursive
for all n by induction on n spec

① Recursive specification

$\text{select}(k, A[1..n])$: Given an array $A[1..n]$ of comparable elements and an integer $k \in \{1, \dots, n\}$, returns the k th smallest element out of $A[1..n]$.

② Implement spec

$\text{multiply}(x[1..n], y[1..n])$

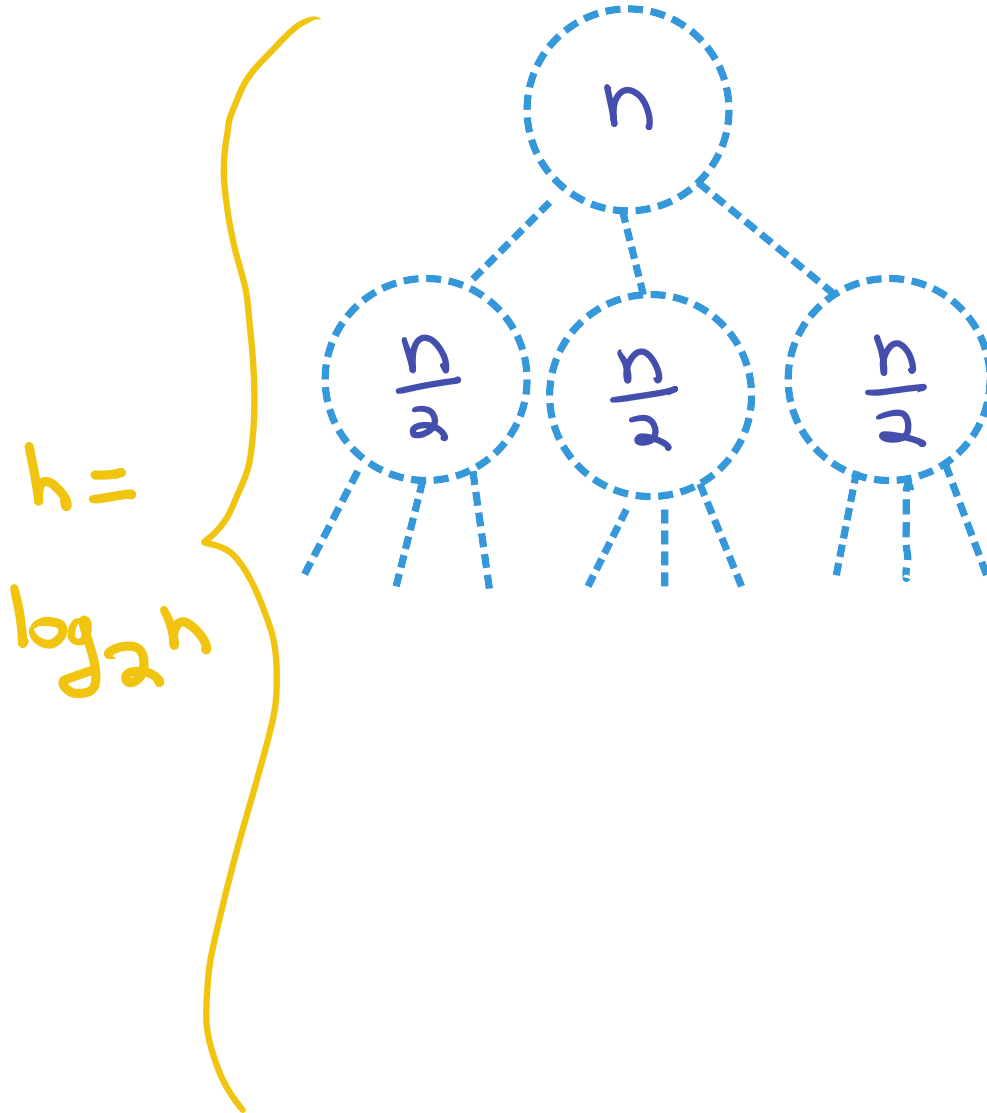
1. If $n = 0$ then return 0.
 2. If $n = 1$ then return $x[1] * y[1]$.
 3. If n is not even then pad x and y with a leading 0, making n even.
// $O(n)$.
 4. Let $x_1 = x[1..n/2]$, $x_2 = [n/2 + 1..n]$, $y_1 = y[1..n/2]$, and $y_2 = y[n/2 + 1..n]$ (as $n/2$ -bit integers).
// $O(n)$.
 5. Let $x_3[1..n/2 + 1] = x_1 + x_2$ and $y_3[1..n/2 + 1] = (y_1 + y_2)$ (as $(n/2 + 1)$ -bit integers).
// $O(n)$.
 6. Let $Z_1 = \text{multiply}(x_1, y_1)$, $Z_2 = \text{multiply}(x_2, y_2)$, and $Z_3 = \text{multiply}(x_3, y_3)$.
// $3T((n + 2)/2)$.
- /* Note that multiplying by 2^n is just a bit-shift and takes $O(n)$ time. */*
7. Return $2^n * Z_1 + 2^{n/2}(Z_3 - Z_1 - Z_2) + Z_2$

4. Running time

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

multiply($x[1..n], y[1..n]$)

1. If $n = 0$ then return 0.
 2. If $n = 1$ then return $x[1] * y[1]$.
 3. If n is not even then pad x and y with a leading 0, making n even.
// $O(n)$.
 4. Let $x_1 = x[1..n/2]$, $x_2 = x[n/2+1..n]$, $y_1 = y[1..n/2]$, and $y_2 = y[n/2+1..n]$ (as $n/2$ -bit integers). // $O(n)$.
 5. Let $x_3[1..n/2+1] = x_1 + x_2$ and $y_3[1..n/2+1] = (y_1 + y_2)$ (as $(n/2+1)$ -bit integers). // $O(n)$.
 6. Let $Z_1 = \text{multiply}(x_1, y_1)$, $Z_2 = \text{multiply}(x_2, y_2)$, and $Z_3 = \text{multiply}(x_3, y_3)$. // $3T((n+2)/2)$.
- /* Note that multiplying by 2^n is just a bit-shift and takes $O(n)$ time. */*
7. Return $2^n * Z_1 + 2^{n/2} (Z_3 - Z_1 - Z_2) + Z_2$



n

$$3 \times \frac{n}{2} = \frac{3}{2}n$$

$$\left(\frac{3}{2}\right)^2 n$$

$\downarrow$

$$\left(\frac{3}{2}\right)^h n$$

Running time

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

$$\begin{aligned} \sum_{i=0}^{\log_2 n} \left(\frac{3}{2}\right)^i n &= O\left(\left(\frac{3}{2}\right)^{\log_2 n} \cdot n\right) \\ &= O(n^{\log_2(3/2) + 1}) \\ &= O(n^{\log_2(3)}) \end{aligned}$$

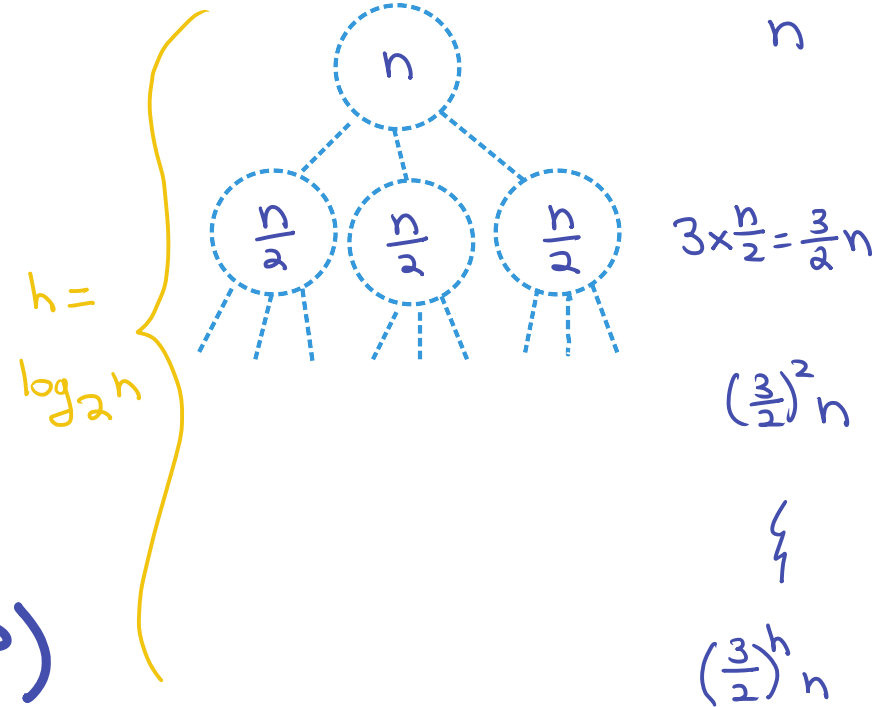
$$T(n) = 3T\left(\frac{n}{2}\right) + O(n) = O(n^{\log_2 3})$$

$$\approx n^{1.585}$$

4. Running time

multiply(x[1..n], y[1..n])

1. If $n = 0$ then return 0.
2. If $n = 1$ then return $x[1] * y[1]$.
3. If n is not even then pad x and y with a leading 0, making n even.
// $O(n)$.
4. Let $x_1 = x[1..n/2]$, $x_2 = [n/2 + 1..n]$, $y_1 = y[1..n/2]$, and $y_2 = y[n/2 + 1..n]$ (as $n/2$ -bit integers). // $O(n)$.
5. Let $x_3[1..n/2 + 1] = x_1 + x_2$ and $y_3[1..n/2 + 1] = (y_1 + y_2)$ (as $(n/2 + 1)$ -bit integers). // $O(n)$.
6. Let $Z_1 = \text{multiply}(x_1, y_1)$, $Z_2 = \text{multiply}(x_2, y_2)$, and $Z_3 = \text{multiply}(x_3, y_3)$. // $3T((n+2)/2)$.
- /* Note that multiplying by 2^n is just a bit-shift and takes $O(n)$ time. */
7. Return $2^n * Z_1 + 2^{n/2}(Z_3 - Z_1 - Z_2) + Z_2$



Integer multiplication
and the
Fast Fourier Transform

Complex numbers $\mathbb{C}$

"imaginary i " satisfying $i^2 = -1$

$a + bi$
"real part" "imaginary part"

• $a + bi$

multiplication:

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$\Rightarrow$ polynomials over $\mathbb{C}$

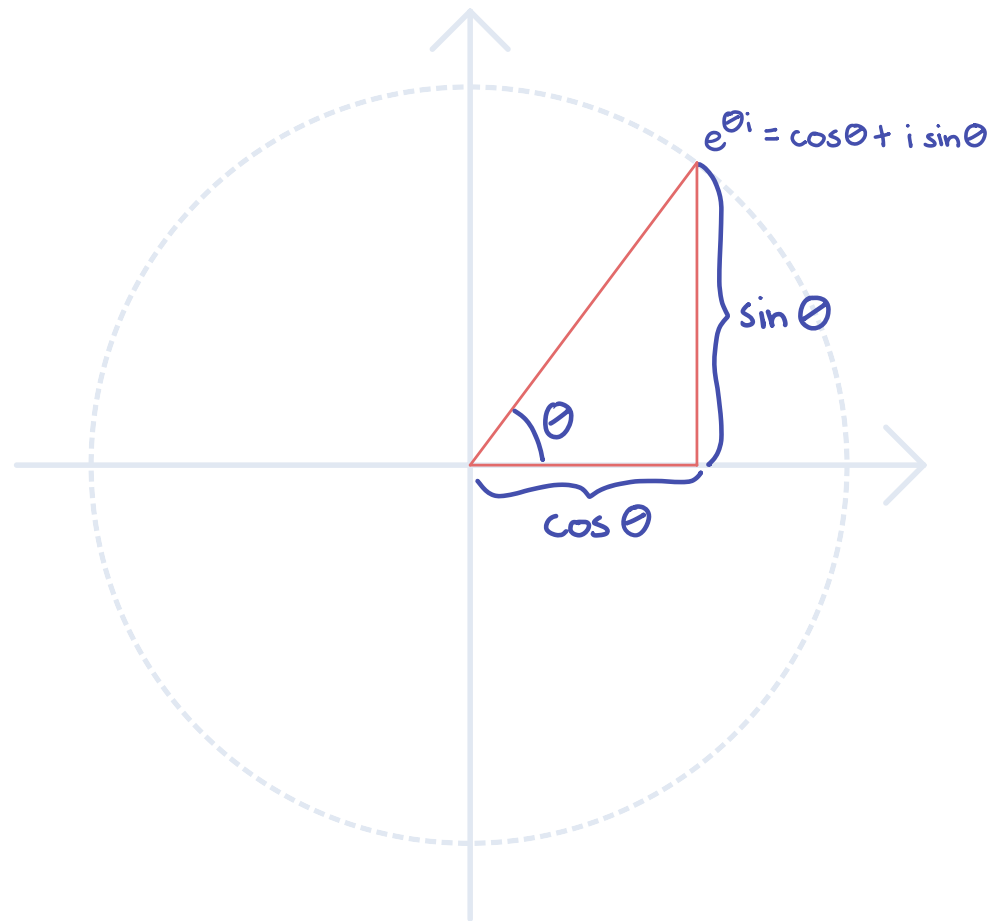
$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$$

$\Rightarrow$ power series over $\mathbb{C}$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula

$$e^{\theta i} = \cos \theta + i \sin \theta$$



$$a + bi$$

"real part"

"imaginary part"

"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

$\Rightarrow$ Euler's identity:

$$\bullet e^{\pi i} = -1$$

$$\bullet e^{2\pi i} = 1$$

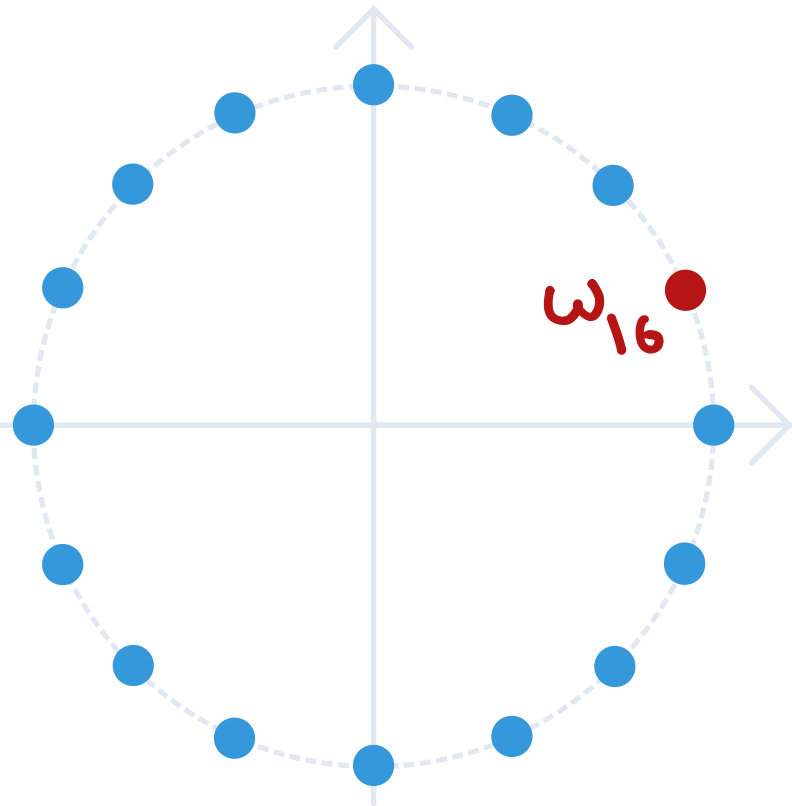
n th roots of unity:

any $w \in \mathbb{C}$ s.t. $w^n = 1$

e.g. $w = 1$ for all n

$w = -1$ for n even

$w = i$ for $n = 4$



let

$$w_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$$1, w_n, w_n^2, \dots, w_n^{n-1}$$

are all n th roots of unity

$$a + bi$$

"real part"

"imaginary part"

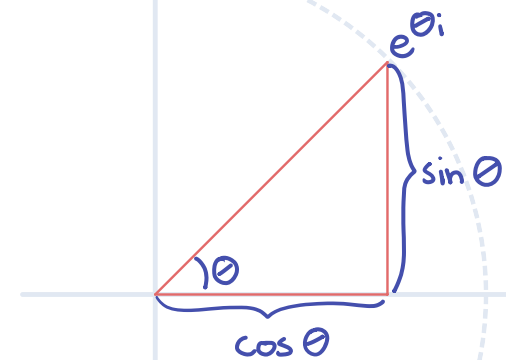
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$e^{\pi i} = -1 \quad e^{2\pi i} = 1$$

(nth) discrete Fourier Transform F_n

Input: $a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{C}$

Output: n values

$$F_n \mathbf{a} = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

conjugate Fourier transform F_n^*

Input: $a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{C}$

Output: n values

$$F_n^* \mathbf{a} = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$a + bi$$

"real part"

"imaginary part"

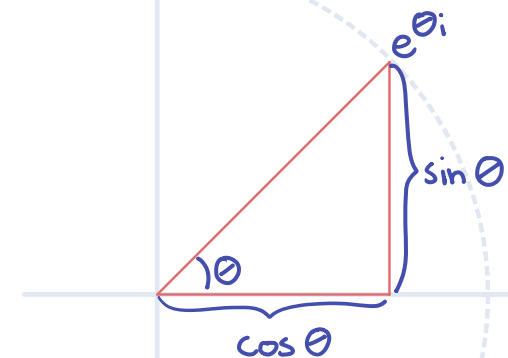
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bc+ad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$e^{\pi i} = -1 \quad e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

Input: $a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{C}$

Output: n values

$$F_n \mathbf{a} = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* \mathbf{a} = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

where $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$

Fact: $F_n^* F_n \mathbf{a} = F_n F_n^* \mathbf{a} = n \mathbf{a}$

(i.e., F_n and F_n^* are essentially inverse)

$$a + bi$$

"real part"

"imaginary part"

"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bc+ad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$e^{\pi i} = -1 \quad e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

Input: $a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{C}$

Output: n values

$$F_n \mathbf{a} = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* \mathbf{a} = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$\text{Fact: } F_n^* F_n \mathbf{a} = F_n F_n^* \mathbf{a} = n \mathbf{a}$$

Theorem: $F_n \mathbf{a}$ and $F_n^* \mathbf{a}$ can be computed in $O(n \log n)$ time.

$$a + bi$$

"real part"

"imaginary part"

"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$e^{\pi i} = -1 \quad e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

Application: multiplying polynomials

$$p(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$$

$$q(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$$

goal: compute

$$r(x) = p(x)q(x)$$

$$= c_0 + c_1x + \dots + c_{2n-2}x^{2n-2}$$

where
$$c_k = \sum_{i=0}^k a_i b_{k-i}$$

$$a + bi$$

"real part"

"imaginary part"

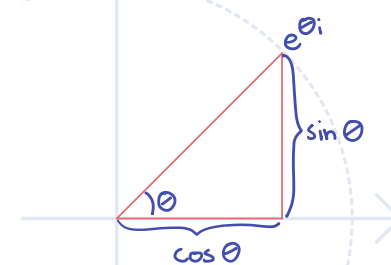
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's Formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$\cdot e^{\pi i} = -1 \quad \cdot e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

where $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$

Fact: $F_n^* F_n a = F_n F_n^* a = na$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Input: $p(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$
 $q(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$

goal: $r(x) = p(x)q(x) = c_0 + c_1x + \dots + c_{2n-2}x^{n-2}$

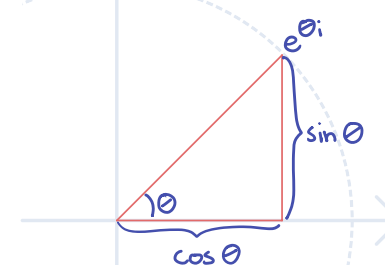
Idea: $r(\omega_{2n}^i) = p(\omega_{2n}^i)q(\omega_{2n}^i)$

(p, q)
 $\downarrow O(n \log n)$
 $(F_{2n}a, F_{2n}b)$
 $\downarrow O(n)$ by mult. pairwise
 $F_{2n}c$
 $\downarrow O(n \log n)$
 $c = \frac{1}{2n} F_{2n}^* F_{2n} c$

$a + bi$
 "real part" "imaginary part"
 "imaginary i " s.t. $i^2 = -1$
 $(a+bi)(c+di) = ac + (bctad)i - bd$
 $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$

Euler's Formula:

$e^{i\theta} = \cos \theta + i \sin \theta$



Euler's identity:

$e^{\pi i} = -1$ $e^{2\pi i} = 1$

$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$
 $F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$
 where $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$

Fact: $F_n^* F_n a = F_n F_n^* a = na$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Input: $a_0, a_1, a_2, \dots, a_{n-1} \in \mathbb{C}$

Output: n values

$$F_n \mathbf{a} = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* \mathbf{a} = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

where $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$

Fact: $F_n^* F_n \mathbf{a} = F_n F_n^* \mathbf{a} = n\mathbf{a}$

Theorem: $F_n \mathbf{a}$ and $F_n^* \mathbf{a}$ can be computed in $O(n \log n)$ time.

$$a + bi$$

"real part"

"imaginary part"

"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$e^{\pi i} = -1 \quad e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

Idea: $\omega_{2n}^2 = \omega_n$

let $a = (a_0, a_1, \dots, a_{2n-1})$.

$$(F_{2n} a)_k = a_0 + a_1 \omega_{2n}^k + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}$$

$$= (a_0 + a_2 (\omega_{2n}^k)^2 + \dots + a_{2n-2} (\omega_{2n}^k)^{2n-2}) \quad (\text{even})$$

$$+ (a_1 \omega_{2n}^k + a_3 (\omega_{2n}^k)^3 + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}) \quad (\text{odd})$$

$a + bi$

"real part"

"imaginary part"

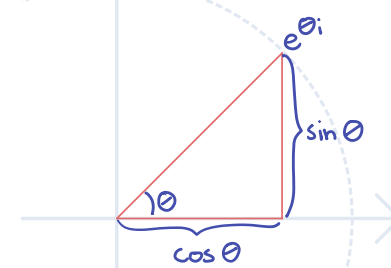
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's Formula:

$$e^{i\theta} = \cos \theta + i \sin \theta$$



Euler's identity:

$$\cdot e^{\pi i} = -1 \cdot e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$\text{Fact: } F_n^* F_n a = F_n F_n^* a = na$$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Idea: $\omega_{2n}^2 = \omega_n$

let $a = (a_0, a_1, \dots, a_{2n-1})$.

$$(F_{2n} a)_k = a_0 + a_1 \omega_{2n}^k + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}$$

$$= (a_0 + a_2 (\omega_{2n}^k)^2 + \dots + a_{2n-2} (\omega_{2n}^k)^{2n-2}) \quad (\text{even})$$

$$+ (a_1 \omega_{2n}^k + a_3 (\omega_{2n}^k)^3 + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}) \quad (\text{odd})$$

$$(a_0 + a_2 (\omega_{2n}^k)^2 + \dots + a_{2n-2} (\omega_{2n}^k)^{2n-2})$$

$$= a_0 + a_2 \omega_n^k + \dots + a_{2n-2} (\omega_n^k)^{n-1}$$

$$= (F_n a_{\text{even}})_k$$

w/ $a_{\text{even}} = (a_0, a_2, \dots, a_{2n-2})$

$a + bi$

"real part"

"imaginary part"

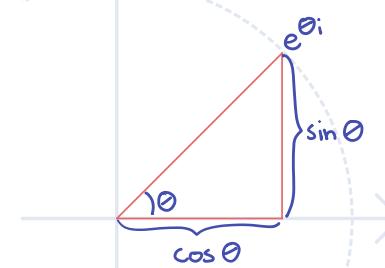
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's Formula:

$$e^{i\theta} = \cos \theta + i \sin \theta$$



Euler's identity:

$$\cdot e^{\pi i} = -1 \cdot e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$\text{Fact: } F_n^* F_n a = F_n F_n^* a = na$$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Idea: $\omega_{2n}^2 = \omega_n$

let $a = (a_0, a_1, \dots, a_{2n-1})$.

$$(F_{2n} a)_k = a_0 + a_1 \omega_{2n}^k + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}$$

$$= (a_0 + a_2 (\omega_{2n}^k)^2 + \dots + a_{2n-2} (\omega_{2n}^k)^{2n-2}) \quad (\text{even})$$

$$+ (a_1 \omega_{2n}^k + a_3 (\omega_{2n}^k)^3 + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}) \quad (\text{odd})$$

$$(a_1 \omega_{2n}^k + a_3 (\omega_{2n}^k)^3 + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}) \quad (\text{odd})$$

$$= \omega_{2n}^k (a_1 + a_3 \omega_n^k + \dots + a_{2n-1} \omega_n^{n-1})$$

$$= \omega_{2n}^k (F_n a_{\text{odd}})_k$$

w/ $a_{\text{odd}} = (a_1, a_3, \dots, a_{2n-1})$

$a + bi$

"real part"

"imaginary part"

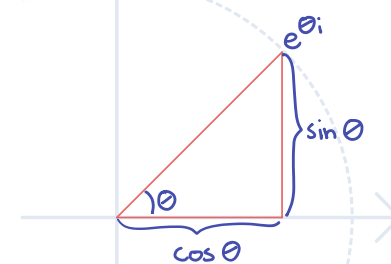
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's Formula:

$$e^{i\theta} = \cos \theta + i \sin \theta$$



Euler's identity:

$$\cdot e^{\pi i} = -1 \cdot e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$\text{Fact: } F_n^* F_n a = F_n F_n^* a = na$$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Idea: $\omega_{2n}^2 = \omega_n$

let $a = (a_0, a_1, \dots, a_{2n-1})$.

$$(F_{2n} a)_k = a_0 + a_1 \omega_{2n}^k + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}$$

$$= (a_0 + a_2 (\omega_{2n}^k)^2 + \dots + a_{2n-2} (\omega_{2n}^k)^{2n-2}) \quad (\text{even})$$

$$+ (a_1 \omega_{2n}^k + a_3 (\omega_{2n}^k)^2 + \dots + a_{2n-1} (\omega_{2n}^k)^{2n-1}) \quad (\text{odd})$$

$$= (F_n a_{\text{even}})_k + \omega_{2n}^k (F_n a_{\text{odd}})_k$$

recurse!

$a + bi$

"real part"

"imaginary part"

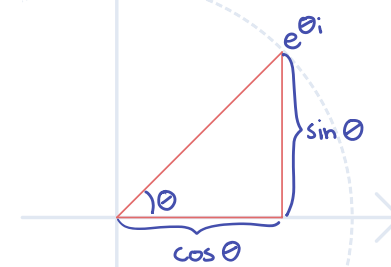
"imaginary i " s.t. $i^2 = -1$

$$(a+bi)(c+di) = ac + (bctad)i - bd$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

Euler's Formula:

$$e^{\theta i} = \cos \theta + i \sin \theta$$



Euler's identity:

$$\cdot e^{\pi i} = -1 \cdot e^{2\pi i} = 1$$

$$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$$

$$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$$

$$\text{where } p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$$

$$\text{Fact: } F_n^* F_n a = F_n F_n^* a = na$$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Fast Fourier Transform ($a_0, \dots, a_n$):

1. if $n=0$ return $\emptyset$
2. if $n=1$ return (a_0)
3. let $(y_0, \dots, y_{n/2-1}) = \text{FFT}(a_{\text{even}})$
4. let $(z_0, \dots, z_{n/2-1}) = \text{FFT}(a_{\text{odd}})$
5. return $(x_0, \dots, x_{n-1})$

where $x_k = y_k + \omega_n^k z_k \quad k=0, \dots, n-1$

$T(n) =$

$a + bi$

"real part"

"imaginary part"

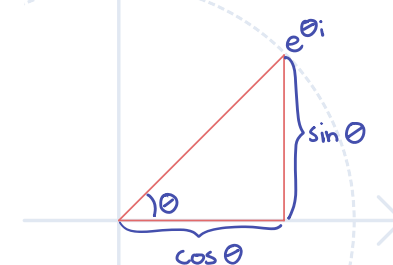
"imaginary i " s.t. $i^2 = -1$

$(a+bi)(c+di) = ac + (bc+ad)i - bd$

$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$

Euler's Formula:

$e^{i\theta} = \cos\theta + i\sin\theta$



Euler's identity:

$\cdot e^{\pi i} = -1 \cdot e^{2\pi i} = 1$

$\omega_n \stackrel{\text{def}}{=} e^{2\pi i/n}$

$1, \omega_n, \omega_n^2, \dots, \omega_n^{n-1}$ are all n th roots of unity

$F_n a = (p(1), p(\omega_n), p(\omega_n^2), \dots, p(\omega_n^{n-1}))$

$F_n^* a = (p(1), p(\omega_n^{n-1}), p(\omega_n^{n-2}), \dots, p(\omega_n))$

where $p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^{n-1}$

Fact: $F_n^* F_n a = F_n F_n^* a = na$

Theorem: $F_n a, F_n^* a$ in $O(n \log n)$

Matrix Multiplication

Let A and B be two $n \times n$ matrices.

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}$$

Write $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$

$$AB = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}$$

(8 multiplies)

Matrix Multiplication

Let A and B be two $n \times n$ matrices.

$$(AB)_{ij} = \sum_k A_{ik} B_{kj}$$

$$AB = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}$$

Strassen, 1969

(8 multiplies)

$$(A_{11} + A_{22})(B_{11} + B_{22}) = A_{11}B_{11} + A_{22}B_{11} + A_{11}B_{22} + A_{22}B_{22} \quad (4.3)$$

$$(A_{11} - A_{21})(B_{11} - B_{12}) = A_{11}B_{11} - A_{21}B_{11} - A_{11}B_{12} + A_{21}B_{12} \quad (4.4)$$

$$(A_{12} - A_{21})(B_{21} + B_{22}) = A_{12}B_{12} - A_{21}B_{21} - A_{21}B_{22} + A_{12}B_{22} \quad (4.5)$$

$$A_{11}(B_{12} - B_{22}) = A_{11}(B_{12} - B_{22}) \quad (4.6)$$

$$(A_{11} + A_{12})B_{22} = A_{11}B_{22} + A_{12}B_{22} \quad (4.7)$$

$$(A_{11} + A_{22})(B_{11} + B_{22}) = A_{11}B_{11} + A_{11}B_{11} + A_{22}B_{11} + A_{22}B_{22} \quad (4.8)$$

$$(A_{11} - A_{21})(B_{11} + B_{12}) = A_{11}B_{11} - A_{21}B_{11} + A_{11}B_{12} - A_{21}B_{12} \quad (4.9)$$

Then

$$\begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix} \\ = \begin{pmatrix} (4.3) + (4.4) - (4.7) + (4.5) & (4.6) + (4.7) \\ (4.8) + (4.4) & (4.6) + (4.3) - (4.8) - (4.9) \end{pmatrix}$$

$$(A_{11} + A_{22})(B_{11} + B_{22}) = A_{11}B_{11} + A_{22}B_{11} + A_{11}B_{22} + A_{11}B_{22} \quad (4.3)$$

$$(A_{11} - A_{21})(B_{11} - B_{12}) = A_{11}B_{11} - A_{21}B_{11} - A_{11}B_{12} + A_{21}B_{12} \quad (4.4)$$

$$(A_{12} - A_{21})(B_{21} + B_{22}) = A_{12}B_{12} - A_{21}B_{21} - A_{21}B_{22} + A_{12}B_{22} \quad (4.5)$$

$$A_{11}(B_{12} - B_{22}) = A_{11}(B_{12} - B_{22}) \quad (4.6)$$

$$(A_{11} + A_{12})B_{22} = A_{11}B_{22} + A_{12}B_{22} \quad (4.7)$$

$$(A_{11} + A_{22})(B_{11} + B_{22}) = A_{11}B_{11} + A_{11}B_{11} + A_{22}B_{11} + A_{22}B_{22} \quad (4.8)$$

$$(A_{11} - A_{21})(B_{11} + B_{12}) = A_{11}B_{11} - A_{21}B_{11} + A_{11}B_{12} - A_{21}B_{12} \quad (4.9)$$

Then

$$\begin{pmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix} \\ = \begin{pmatrix} (4.3) + (4.4) - (4.7) + (4.5) & (4.6) + (4.7) \\ (4.8) + (4.4) & (4.6) + (4.3) - (4.8) - (4.9) \end{pmatrix}$$

$T(n) =$