CSL 356: Analysis and Design of Algorithms

Ragesh Jaiswal

CSE, IIT Delhi

Divide and Conquer: Examples

Fast Fourier Transform (FFT)

Divide and Conquer: Examples

- Problem: Given two polynomials

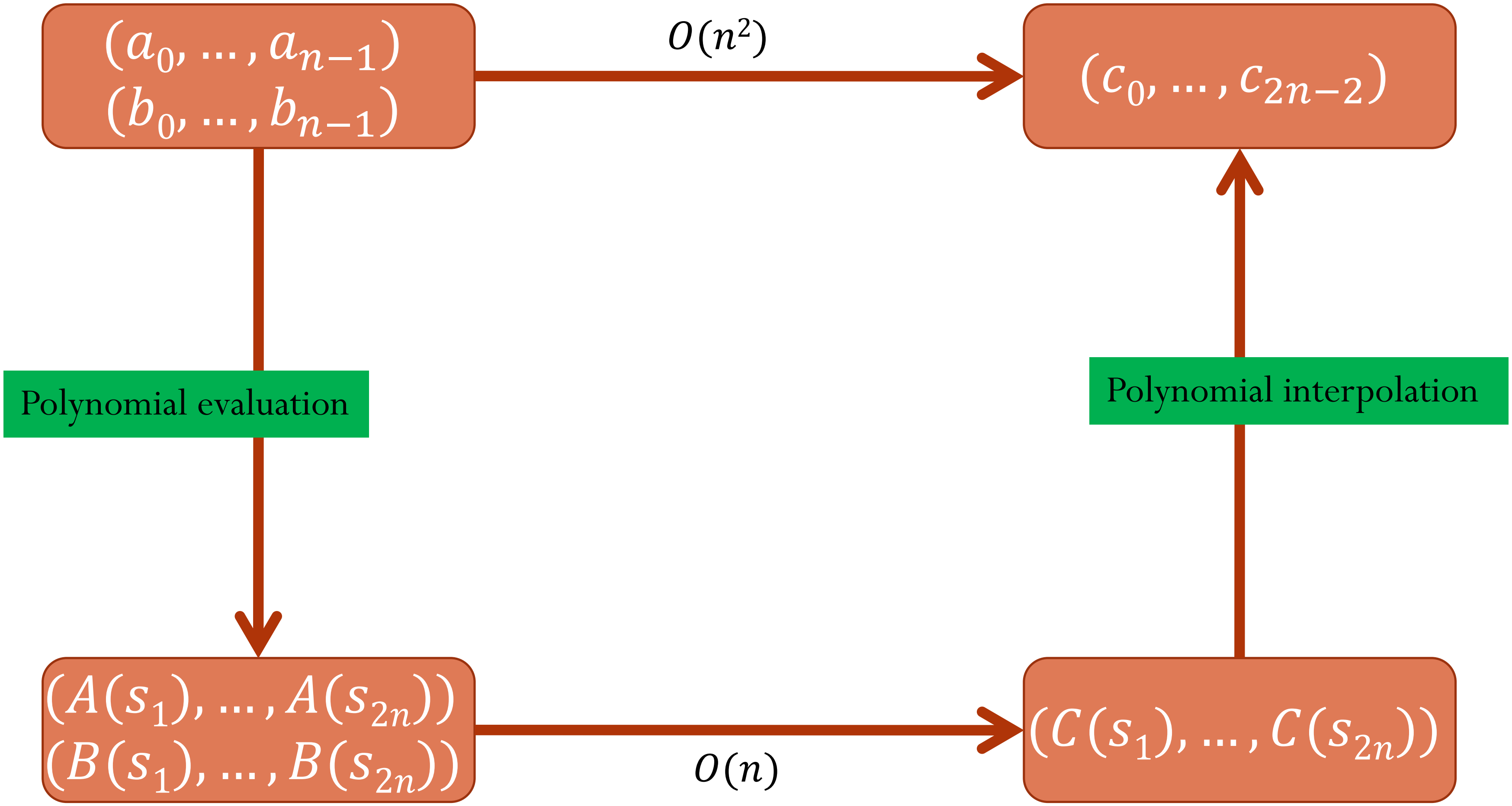
  $$A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{n-1} \cdot x^{n-1},$$

  and

  $$B(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \ldots + b_{n-1} \cdot x^{n-1}$$

  multiply them.

Divide and Conquer: Examples



Divide and Conquer: Examples

- <u>Polynomial interpolation</u>: We have $(C(s_1), \ldots, C(s_{2n}))$ and we need to compute $(c_0, \ldots, c_{2n-2})$.

$$
\begin{bmatrix}
1 & s_1 & (s_1)^2 & \cdots & (s_1)^{2n-1} \\
1 & s_2 & (s_2)^2 & \cdots & (s_2)^{2n-1} \\
1 & S_3 & (s_3)^2 & \cdots & (s_3)^{2n-1} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
1 & S_{2n} & (s_{2n})^2 & \cdots & (s_{2n})^{2n-1}
\end{bmatrix}
*
\begin{bmatrix}
c_0 \\ c_1 \\ c_2 \\ \cdots \\ c_{2n-1}
\end{bmatrix}
=
\begin{bmatrix}
C(s_1) \\ C(s_2) \\ C(s_3) \\ \cdots \\ C(s_{2n})
\end{bmatrix}
$$

- Is the above square matrix invertible?

Divide and Conquer: Examples

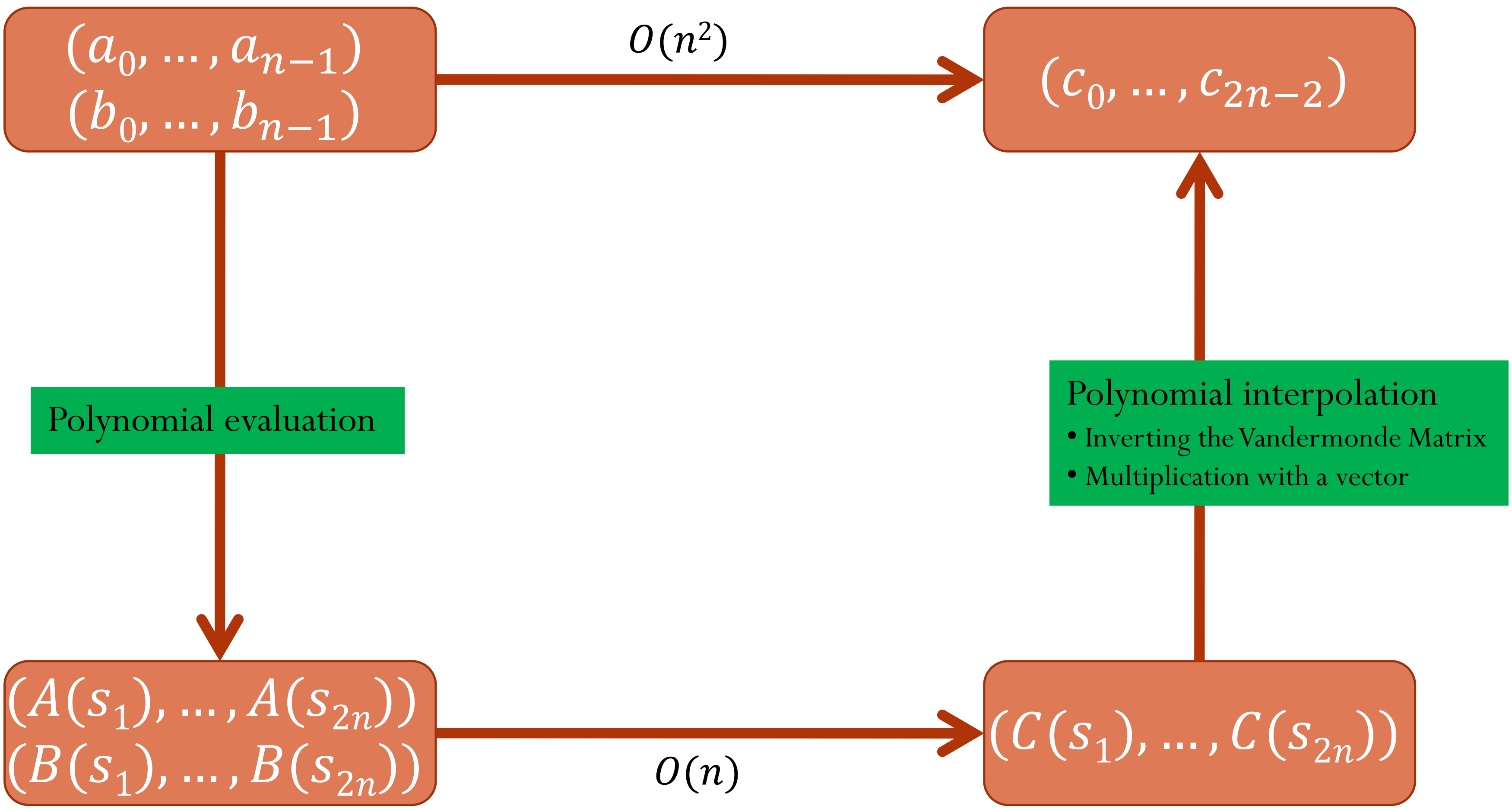
- A square matrix is invertible iff its determinant is non-zero.
- The matrix shown below has a special name: *Vandermonde Matrix*.
  - Claim: $Det(V) = \prod_{1 \le j < i \le 2n} (s_i - s_j)$

1	s_1	$(s_1)^2$	…	$(s_1)^{2n-1}$
1	s_2	$(s_2)^2$	…	$(s_2)^{2n-1}$
1	S_3	$(s_3)^2$	…	$(s_3)^{2n-1}$
…	…	…	…	…
1	S_{2n}	$(s_{2n})^2$	…	$(s_{2n})^{2n-1}$

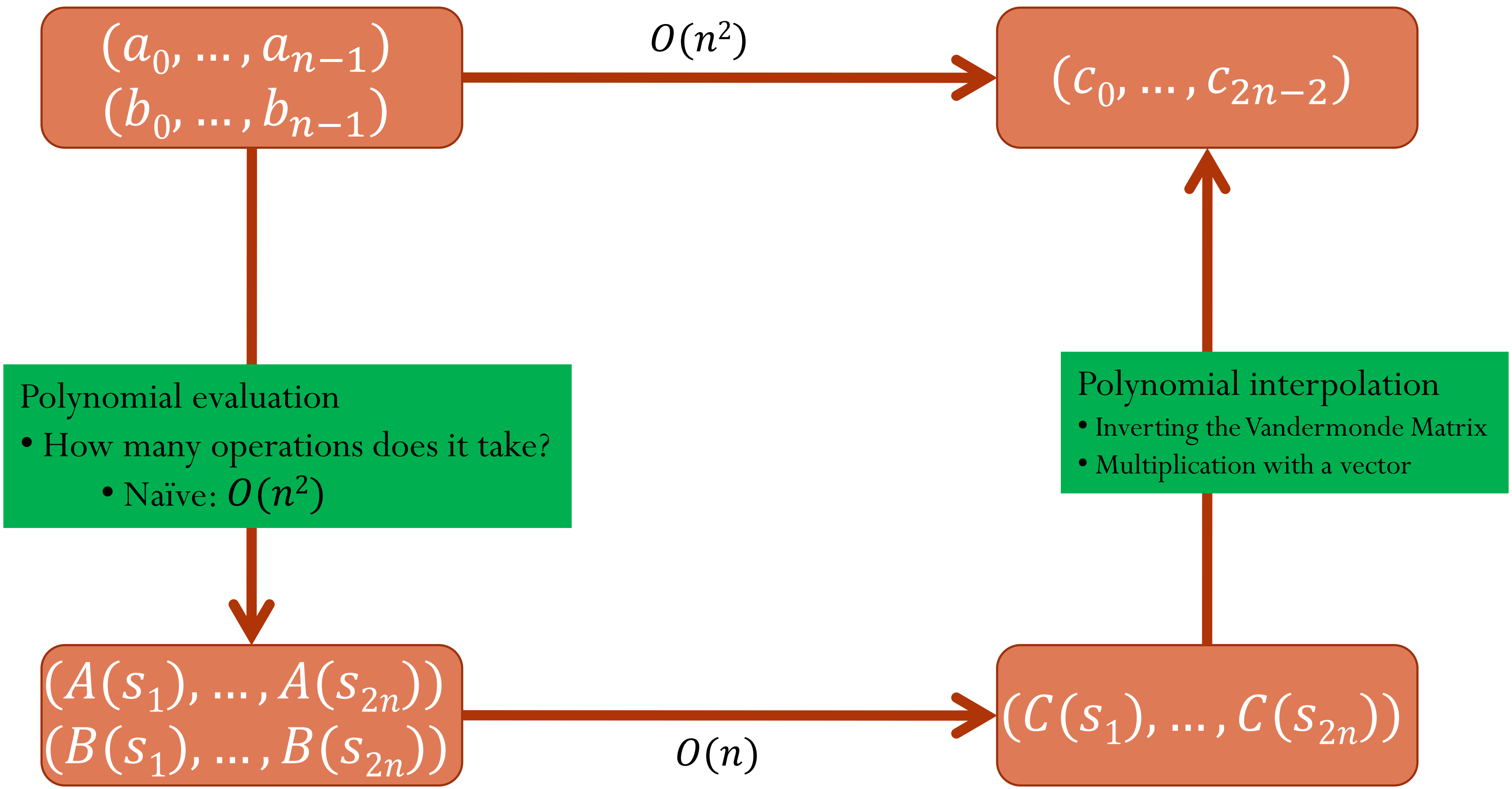
Divide and Conquer: Examples

- A square matrix is invertible iff its determinant is non-zero.
- The matrix shown below has a special name: *Vandermonde Matrix*.
  - Claim: $$Det(V) = \prod_{1 \le j < i \le 2n} (s_i - s_j)$$
- So, as long as we use distinct values of $s_1, \ldots, s_{2n}$, we will be able to do polynomial interpolation.

Divide and Conquer: Examples



Divide and Conquer: Examples



Divide and Conquer: Examples

- Example:
  - $A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 + 2x^6 + x^7$
  - $A(x) = (3 + 6x^2 + x^4 + 2x^6) + x(4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(x) = (3 + 6x^2 + x^4 + 2x^6)$
  - $A_1(x) = (4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(1) = 12, A_1(1) = 17$, so $A(1) = 12 + 1 * 17 = 29$
  - What is $A(-1)$?

Divide and Conquer: Examples

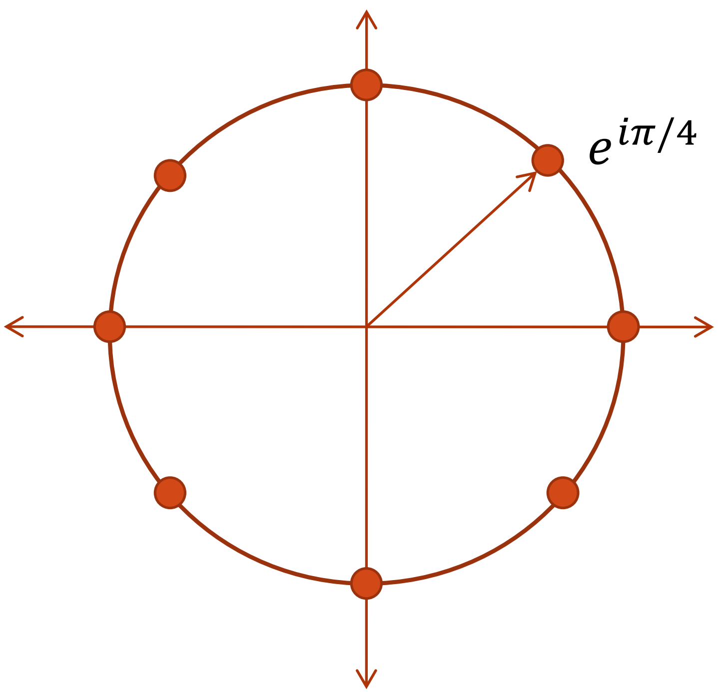
- <u>Example</u>:
  - $A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 + 2x^6 + x^7$
  - $A(x) = (3 + 6x^2 + x^4 + 2x^6) + x(4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(x) = (3 + 6x^2 + x^4 + 2x^6)$
  - $A_1(x) = (4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(1) = 12, A_1(1) = 17$, so $A(1) = 12 + 1 * 17 = 29$
  - What is $A(-1)$?
    - $A(-1) = A_0(-1) + -1 \cdot A_1(-1)$
      $= A_0(1) + -1 \cdot A_1(1)$
      $= 12 - 17 = -5$

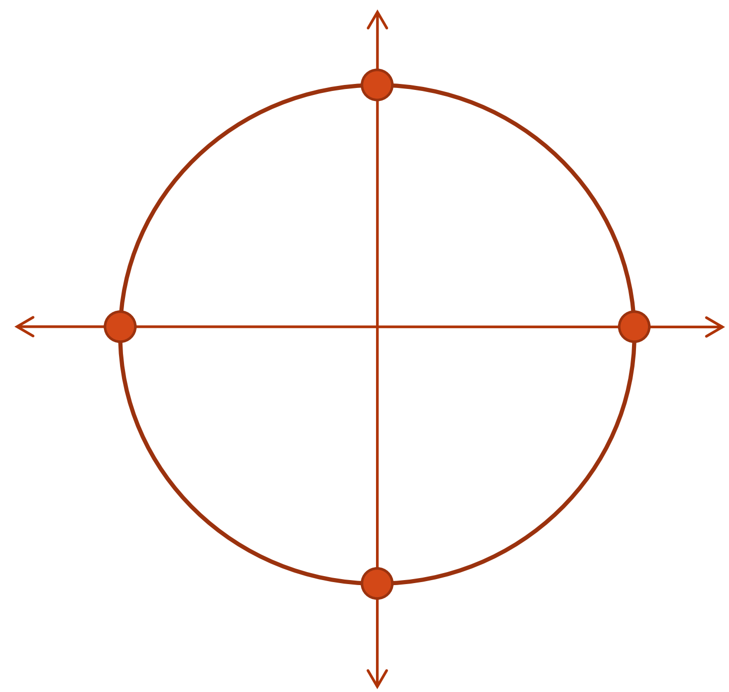
Divide and Conquer: Examples

- <u>Example</u>:
  - $A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 + 2x^6 + x^7$
  - $A(x) = (3 + 6x^2 + x^4 + 2x^6) + x(4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(x) = (3 + 6x^2 + x^4 + 2x^6)$
  - $A_1(x) = (4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(1) = 12, A_1(1) = 17$, so $A(1) = 12 + 1 * 17 = 29$
  - What is $A(-1)$?
    - $$\begin{aligned} A(-1) &= A_0(-1) + -1 \cdot A_1(-1) \\ &= A_0(1) + -1 \cdot A_1(1) \\ &= 12 - 17 = -5 \end{aligned}$$
  - If we want to compute A on $-1,1,-2,2,-3,3,-4,4$ then we need to compute A_0 and A_1 on only $1,2,3,4$.

Divide and Conquer: Examples

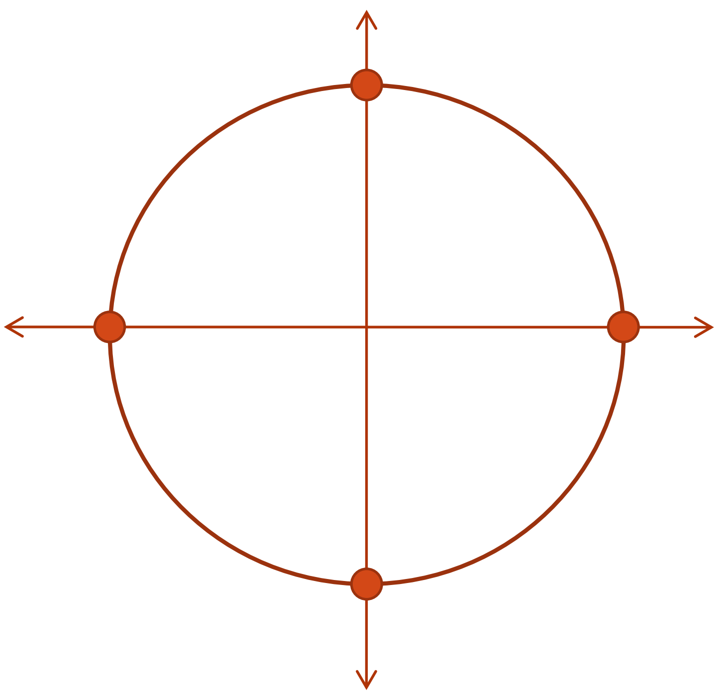
- <u>Example</u>:
  - $A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 + 2x^6 + x^7$
  - $A(x) = (3 + 6x^2 + x^4 + 2x^6) + x \cdot (4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(x) = (3 + 6x^2 + x^4 + 2x^6)$
  - $A_1(x) = (4 + 2x^2 + 10x^4 + x^6)$

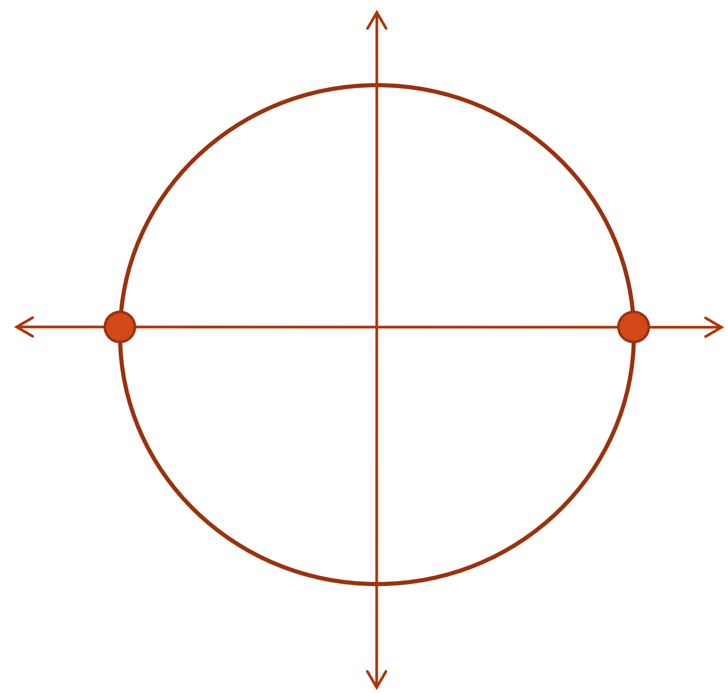




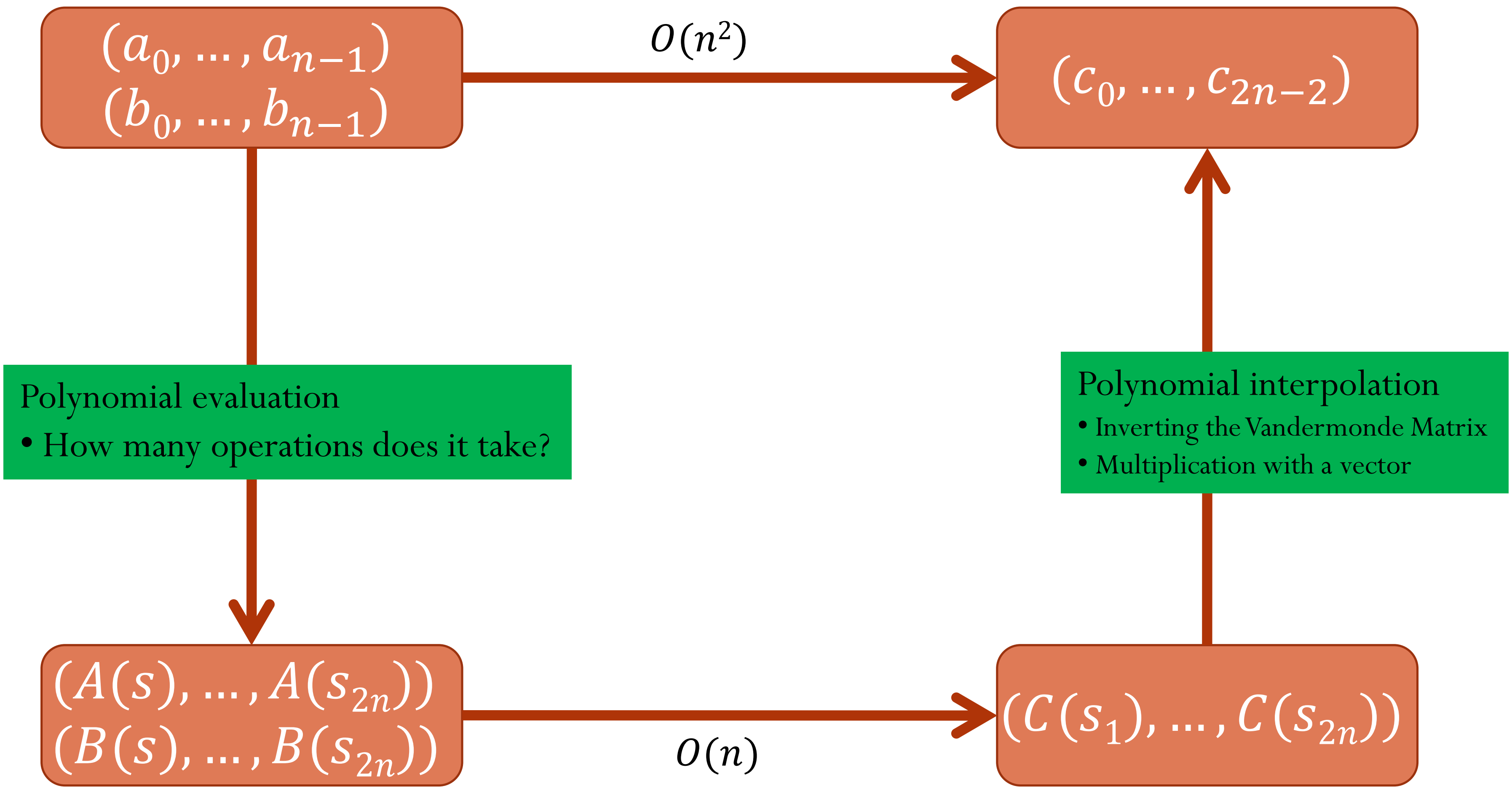
Divide and Conquer: Examples

- Example:
  - $A(x) = 3 + 4x + 6x^2 + 2x^3 + x^4 + 10x^5 + 2x^6 + x^7$
  - $A(x) = (3 + 6x^2 + x^4 + 2x^6) + x(4 + 2x^2 + 10x^4 + x^6)$
  - $A_0(x) = (3 + 6x^2 + x^4 + 2x^6)$
  - $A_1(x) = (4 + 2x^2 + 10x^4 + x^6)$
  - $A_{00}(x) = (3 + x^4), A_{01}(x) = (6 + 2x^4)$
  - $A_{10}(x) = (4 + 10x^4), A_{11}(x) = (2 + x^4)$





Divide and Conquer: Examples



Divide and Conquer: Examples

- Can we choose $s_1, \dots, s_{2n}$ in a more clever manner so that evaluating the polynomials A and B on these points cost fewer operations?
- We will use complex roots of unity!
  - We will use the $2n$ roots of the equation
  $$x^{2n} - 1 = 0$$
  - $s_1 = e^{1 \cdot 2i\pi/2n}$,
  - $s_1 = e^{2 \cdot 2i\pi/2n}$,
  - …
  - $sj = e^{j \cdot 2i\pi/2n}$,
  - …

Divide and Conquer: Examples

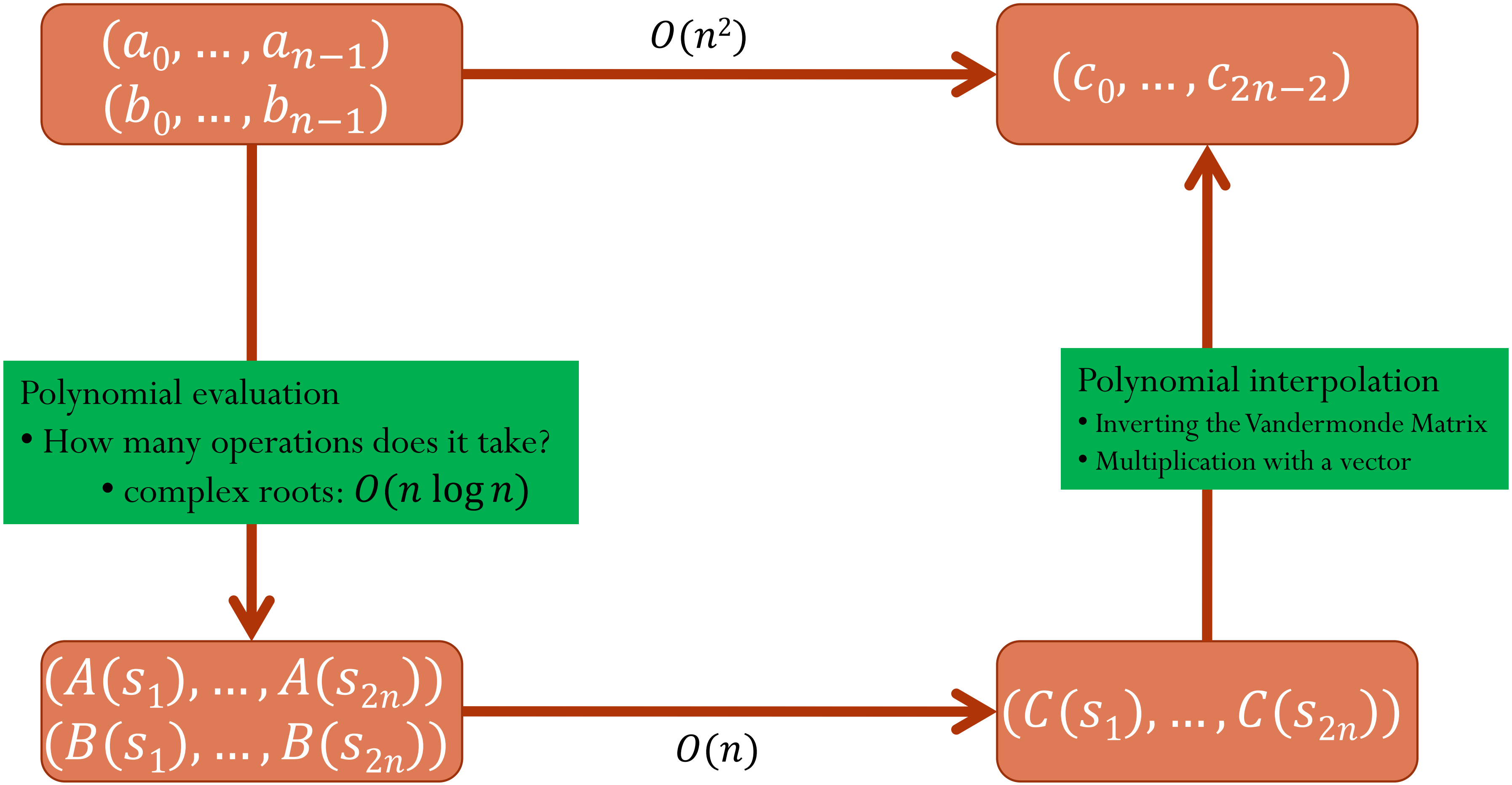
- Let w be one of the $2n$ roots of unity.
- $A(w) = (a_0 + a_2 \cdot w^2 + a_4 \cdot w^4 + \cdots) + w \cdot (a_1 + a_3 \cdot w^2 + a_5 \cdot w^4 + \cdots)$
  $= A_{even(w^2)} + w \cdot A_{odd}(w^2)$
- If we have $A_{even}(w^2)$ and $A_{odd}(w^2)$, the computing $A(w)$ takes constant number of operations.
- Suppose $T(n)$ denotes the worst case time to compute a polynomial at **all** the $2n$ roots of unity.
- Using the above equation, can we say that:

$$T(n) = 2 \cdot T(n/2) + O(n)$$

Divide and Conquer: Examples

- Let w be one of the $2n$ roots of unity.
- $A(w) = (a_0 + a_2 \cdot w^2 + a_4 \cdot w^4 + \cdots) + w \cdot (a_1 + a_3 \cdot w^2 + a_5 \cdot w^4 + \cdots)$
  $$= A_{even(w^2)} + w \cdot A_{odd}(w^2)$$
- If we have $A_{even}(w^2)$ and $A_{odd}(w^2)$, the computing $A(w)$ takes constant number of operations.
- Suppose $T(n)$ denotes the worst case time to compute a polynomial at **all** the $2n$ roots of unity.
- Using the above equation, can we say that:
  $$T(n) = 2 \cdot T(n/2) + O(n)$$
  - Since w^2 is one of the n^{th} roots of unity.

Divide and Conquer: Examples



Divide and Conquer: Examples

- Claim: Let $w = e^{2\pi i/2n}$. Let V be the Vandermonde matrix w.r.t. the $2n$ roots of unity.

1	1	1	…	1
1	w	$(w)2$	…	$(w)^{2n-1}$
1	w^2	$(w^2)^2$	…	$(w^2)^{2n-1}$
…	…	…	…	…
1	w^{2n-1}	$(w^{2n-1})^2$	…	$(w^{2n-1})^{2n-1}$

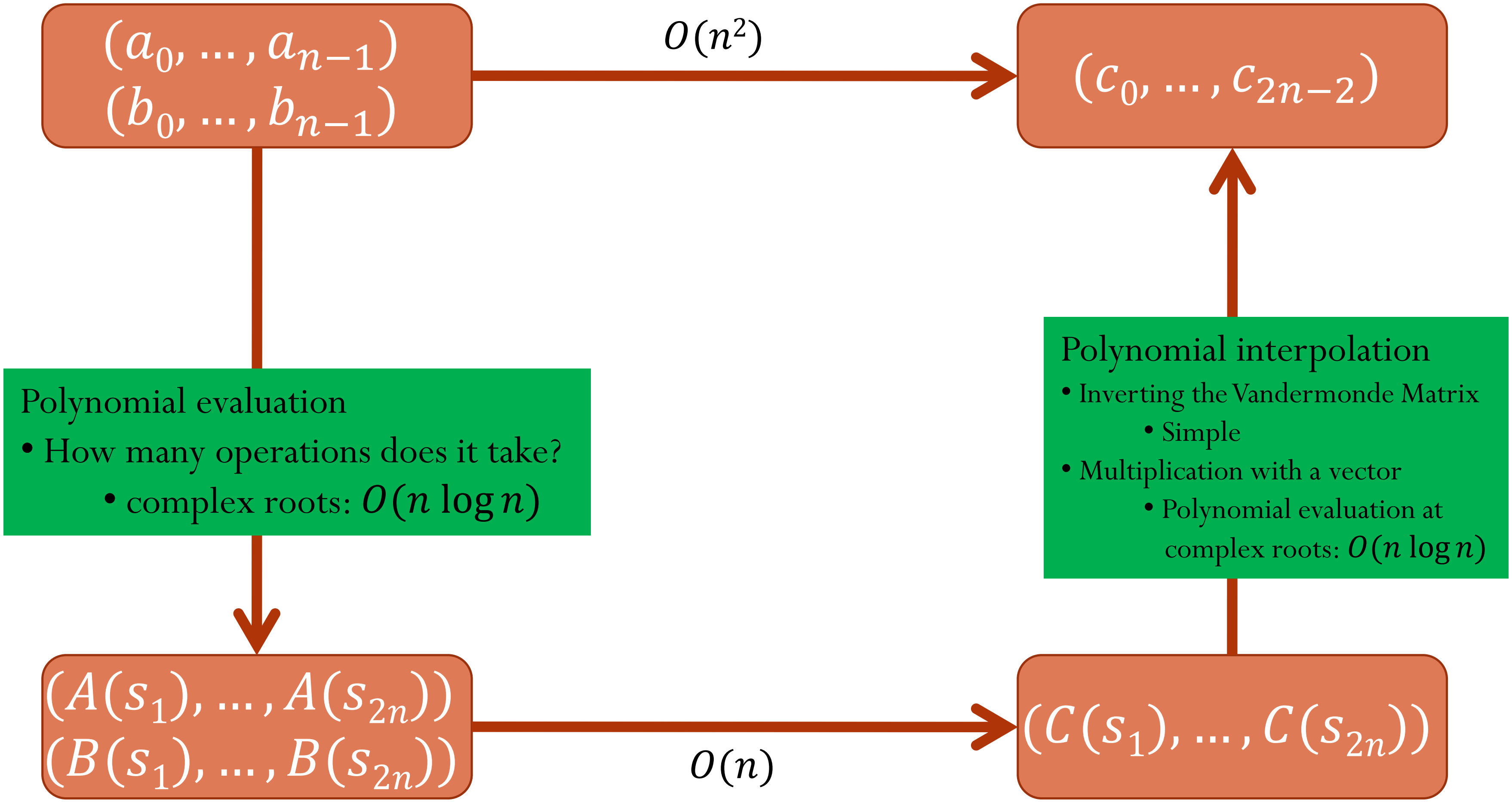
Then, $[V^{-1}]_{ij} = w^{-ij}/(2n)$.

Divide and Conquer: Examples

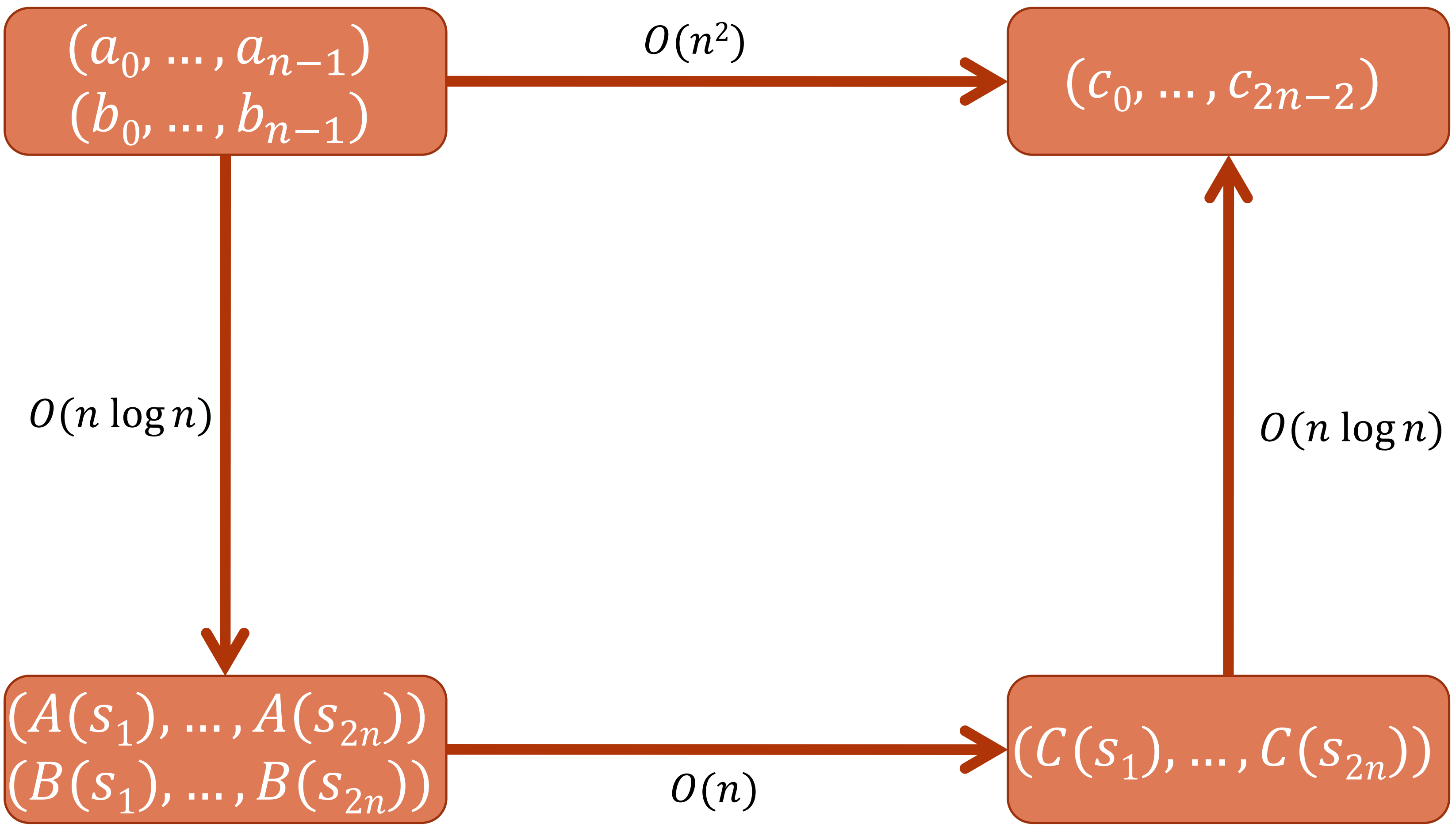
$$V^{-1} = \left(\frac{1}{2n}\right) \cdot \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w^{-1} & (w^{-1})^2 & \dots & (w^{-1})^{2n-1} \\ 1 & w^{-2} & (w^{-2})^2 & \dots & (w^{-2})^{2n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & w^{-(2n-1)} & (w^{-(2n-1)})^2 & \dots & (w^{-(2n-1)})^{2n-1} \end{pmatrix}$$

- $V \cdot (c_0, c_1, \dots, c_{2n-1})^T = (C(1), C(w), \dots, C(w^{2n-1}))^T$
- How do we compute c_i?

Divide and Conquer: Examples



Divide and Conquer: Examples



End