Algorithms and datastructures II

Lecture 7: Fast Fourier Transform 1/2

Jan Hubička

Department of Applied Mathematics
Charles University
Prague

Nov 16 2020

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.
Normal form of a polynomial is created by removing trailing zero coefficients.

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.
Normal form of a polynomial is created by removing trailing zero coefficients.
Multiplication of polynomials is defined as:

$$P(x) \cdot Q(x) = \left(\sum_{i=0}^{n-1} p_i \cdot x^i\right) \cdot \left(\sum_{i=0}^{m-1} q_i \cdot x^i\right) = \sum_{i,j} p_i q_j x^{i+j}.$$

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.
Normal form of a polynomial is created by removing trailing zero coefficients.
Multiplication of polynomials is defined as:

$$P(x) \cdot Q(x) = \left(\sum_{i=0}^{n-1} p_i \cdot x^i \right) \cdot \left(\sum_{i=0}^{m-1} q_i \cdot x^i \right) = \sum_{i,j} p_i q_j x^{i+j}.$$

Result of the multiplication is a polynomial $R(x)$ with

$$r_k = p_0 q_k + p_1 q_{k-1} + \cdots + p_k q_0.$$

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \dots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.
Normal form of a polynomial is created by removing trailing zero coefficients.
Multiplication of polynomials is defined as:

$$P(x) \cdot Q(x) = \left(\sum_{i=0}^{n-1} p_i \cdot x^i\right) \cdot \left(\sum_{i=0}^{m-1} q_i \cdot x^i\right) = \sum_{i,j} p_i q_j x^{i+j}.$$

Result of the multiplication is a polynomial $R(x)$ with

$$r_k = p_0 q_k + p_1 q_{k-1} + \cdots + p_k q_0.$$

Observation

Polynomial $R(x) = P(x) \cdot Q(x)$ can be computed in $\Theta(n^2)$ where $n = |P| = |Q|$.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Lemma

Let $x_0, \ldots, x_d$ by any sequence of distinct numbers. Let P and Q be polynomials of degree at most d. If $P(x_i) = Q(x_i)$ for every $i = 0, 1, \ldots d$ then P and Q are equivalent.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Lemma

Let $x_0, \ldots, x_d$ by any sequence of distinct numbers. Let P and Q be polynomials of degree at most d. If $P(x_i) = Q(x_i)$ for every $i = 0, 1, \ldots d$ then P and Q are equivalent.

Recall:

Lemma

Non-zero polynomial R of degree $t \geq 0$ has at most t roots.

division of polynomials: $R(x) \equiv (x - \alpha) \cdot R'(x) + \beta$ for constant β. If α is root then $\beta = 0$.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Lemma

Let $x_0, \ldots, x_d$ by any sequence of distinct numbers. Let P and Q be polynomials of degree at most d. If $P(x_i) = Q(x_i)$ for every $i = 0, 1, \ldots d$ then P and Q are equivalent.

Recall:

Lemma

Non-zero polynomial R of degree $t \geq 0$ has at most t roots.

division of polynomials: $R(x) \equiv (x - \alpha) \cdot R'(x) + \beta$ for constant β. If α is root then $\beta = 0$.
Now consider $R(x) \equiv P(x) - Q(x)$. Degree of R is at most d and all of $x_0, \ldots, x_d$ are roots.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Lemma

Let $x_0, \ldots, x_d$ by any sequence of distinct numbers. Let P and Q be polynomials of degree at most d. If $P(x_i) = Q(x_i)$ for every $i = 0, 1, \ldots d$ then P and Q are equivalent.

Recall:

Lemma

Non-zero polynomial R of degree $t \geq 0$ has at most t roots.

division of polynomials: $R(x) \equiv (x - \alpha) \cdot R'(x) + \beta$ for constant β. If α is root then $\beta = 0$.
Now consider $R(x) \equiv P(x) - Q(x)$. Degree of R is at most d and all of $x_0, \ldots, x_d$ are roots.

We established bijection between polynomials and vectors of values.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + (p_1 x^1 + p_3 x^3 + \cdots + p_{n-1} x^{n-1})$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

$$P_e(t) = p_0t^0 + p_2t^1 + \cdots + p_{n-2}t^{\frac{n-2}{2}}$$

$$P_o(t) = p_1t^0 + p_3t^1 + \cdots + p_{n-2}t^{\frac{n-1}{2}}$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

$$\begin{aligned} P_e(t) &= p_0t^0 + p_2t^1 + \cdots + p_{n-2}t^{\frac{n-2}{2}} \\ P_o(t) &= p_1t^0 + p_3t^1 + \cdots + p_{n-2}t^{\frac{n-1}{2}} \end{aligned}$$

also

$$P(-x) = P_e(x^2) - xP_o(x^2).$$

We can choose $x_0, -x_0, x_1, -x_1, \ldots x_{n/2}, -x_{n/2}$; evaluate P_e and P_i in $n/2$ points and combine them.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

$$\begin{aligned} P_e(t) &= p_0t^0 + p_2t^1 + \cdots + p_{n-2}t^{\frac{n-2}{2}} \\ P_o(t) &= p_1t^0 + p_3t^1 + \cdots + p_{n-2}t^{\frac{n-1}{2}} \end{aligned}$$

also

$$P(-x) = P_e(x^2) - xP_o(x^2).$$

We can choose $x_0, -x_0, x_1, -x_1, \ldots x_{n/2}, -x_{n/2}$; evaluate P_e and P_i in $n/2$ points and combine them.
Can we get algorithm with time complexity: $T(n) = 2T(n/2) + \Theta(n)$?

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

operations:

1. addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i$
2. subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i$

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

operations:

1. addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i$
2. subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i$
3. multiplication: $(a + bi) \cdot (p + qi) = (ap - bq) + (bq + bp)i$

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

operations:

1. addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i$
2. subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i$
3. multiplication: $(a + bi) \cdot (p + qi) = (ap - bq) + (bq + bp)i$
4. complex conjugate: $\overline{a + bi} = a - bi$

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

operations:

1. addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i$
2. subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i$
3. multiplication: $(a + bi) \cdot (p + qi) = (ap - bq) + (bq + bp)i$
4. complex conjugate: $\overline{a + bi} = a - bi$
5. norm: $|x| = \sqrt{x\overline{x}}$ or $|a + bi| = \sqrt{(a + bi)(a - bi)} = \sqrt{a^2 - b^2}$.

Complex numbers: algebraic approach

Definition (Complex numbers)

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

operations:

1. addition: $(a + bi) + (p + qi) = (a + p) + (b + q)i$
2. subtraction: $(a + bi) - (p + qi) = (a - p) + (b - q)i$
3. multiplication: $(a + bi) \cdot (p + qi) = (ap - bq) + (bq + bp)i$
4. complex conjugate: $\overline{a + bi} = a - bi$
5. norm: $|x| = \sqrt{x\overline{x}}$ or $|a + bi| = \sqrt{(a + bi)(a - bi)} = \sqrt{a^2 - b^2}$.
6. division: apply a trick:
$$\frac{x}{y} = \frac{(x \cdot \overline{y})}{(y \cdot \overline{y})}.$$

   $y\overline{y}$ is real number so we can divide as usual.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i\sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i \sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i\sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.
5. Euler formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i \sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.
5. Euler formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$.
6. Multiplication: $xy = (|x| \cdot e^{i\varphi(x)}).(|y| \cdot e^{i\varphi(y)}) = |x| \cdot |y| \cdot e^{i(\varphi(x)+\varphi(y))}$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i\sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.
5. Euler formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$.
6. Multiplication: $xy = (|x| \cdot e^{i\varphi(x)}).(|y| \cdot e^{i\varphi(y)}) = |x| \cdot |y| \cdot e^{i(\varphi(x)+\varphi(y))}$.
7. Powers: For $\alpha \in \mathbb{R}$: $x^\alpha = \left(|x| \cdot e^{i\varphi(x)}\right)^\alpha = |x|^\alpha \cdot e^{i\alpha\varphi(x)}$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i\sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.
5. Euler formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$.
6. Multiplication: $xy = (|x| \cdot e^{i\varphi(x)}).(|y| \cdot e^{i\varphi(y)}) = |x| \cdot |y| \cdot e^{i(\varphi(x)+\varphi(y))}$.
7. Powers: For $\alpha \in \mathbb{R}$: $x^\alpha = \left(|x| \cdot e^{i\varphi(x)}\right)^\alpha = |x|^\alpha \cdot e^{i\alpha\varphi(x)}$.
8. Roots: For $\alpha \in \mathbb{R}$: $\sqrt[n]{x} = |x|^{1/n} e^{i\varphi(x)/n}$.

Complex numbers: geometric approach

We can assign complex numbers to points in a plane $\mathbb{R}^2$:

$$a + bi \iff (a, b)$$

1. $|x|$ is the distance of x from 0.
2. All values $|x| = 1$ lies on a unit circle
3. For every $x \in \mathbb{C}$: $x = |x|(\cos\varphi(x) + i\sin\varphi(x))$
   $\varphi(x)$ is called argument. It is common to normalize it in interval $[0, 2\pi)$.
4. $\varphi(\overline{x}) = -\varphi(x) \mod 2\pi$.
5. Euler formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$.
6. Multiplication: $xy = (|x| \cdot e^{i\varphi(x)}).(|y| \cdot e^{i\varphi(y)}) = |x| \cdot |y| \cdot e^{i(\varphi(x)+\varphi(y))}$.
7. Powers: For $\alpha \in \mathbb{R}$: $x^\alpha = \left(|x| \cdot e^{i\varphi(x)}\right)^\alpha = |x|^\alpha \cdot e^{i\alpha\varphi(x)}$.
8. Roots: For $\alpha \in \mathbb{R}$: $\sqrt[n]{x} = |x|^{1/n} e^{i\varphi(x)/n}$.

Good news: There exist n distinct values $x_1, x_2, \ldots x_n$ such that $x_i^n = 1$.

Definition (Primitive roots)

x is n-th primitive root of z iff $x^n = z$ and $x^1, \ldots, x^{n-1} \neq z$.

Definition (Primitive roots)

x is n-th primitive root of z iff $x^n = z$ and $x^1, \ldots, x^{n-1} \neq z$.

Example:

$$\omega = e^{\frac{i2\pi}{n}}$$

ω is n-th primitive power of 1.

Definition (Primitive roots)

x is n-th primitive root of z iff $x^n = z$ and $x^1, \ldots, x^{n-1} \neq z$.

Example:

$$\omega = e^{\frac{i2\pi}{n}}$$

ω is n-th primitive power of 1.

Observation

For n even $\omega^{n/2} = -1$.

Definition (Primitive roots)

x is n-th primitive root of z iff $x^n = z$ and $x^1, \ldots, x^{n-1} \neq z$.

Example:

$$\omega = e^{\frac{i2\pi}{n}}$$

ω is n-th primitive power of 1.

Observation

For n even $\omega^{n/2} = -1$.

Observation

For n even ω^2 is $n/2$-th primitive root of 1.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + (p_1 x^1 + p_3 x^3 + \cdots + p_{n-1} x^{n-1})$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \dots, x_{n-1}$.
2. Compute $(P(x_0), \dots, P(x_{n-1}))$ and $(Q(x_0), \dots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \dots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + (p_1 x^1 + p_3 x^3 + \cdots + p_{n-1} x^{n-1}) = P_e(x^2) + x P_o(x^2).$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + (p_1 x^1 + p_3 x^3 + \cdots + p_{n-1} x^{n-1}) = P_e(x^2) + x P_o(x^2).$$

$$\begin{aligned} P_e(t) &= p_0 t^0 + p_2 t^1 + \cdots + p_{n-2} t^{\frac{n-2}{2}} \\ P_o(t) &= p_1 t^0 + p_3 t^1 + \cdots + p_{n-1} t^{\frac{n-2}{2}} \end{aligned}$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

$$\begin{aligned} P_e(t) &= p_0t^0 + p_2t^1 + \cdots + p_{n-2}t^{\frac{n-2}{2}} \\ P_o(t) &= p_1t^0 + p_3t^1 + \cdots + p_{n-1}t^{\frac{n-2}{2}} \end{aligned}$$

also

$$P(-x) = P_e(x^2) - xP_o(x^2).$$

WLOG $n = 2^k$ and evaluate in $\omega^0, \omega^1, \ldots, \omega^{n-1}$.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Can we use divide and conquer to do step 2 effectively?

$$P(x) = (p_0x^0 + p_2x^2 + \cdots + p_{n-2}x^{n-2}) + (p_1x^1 + p_3x^3 + \cdots + p_{n-1}x^{n-1}) = P_e(x^2) + xP_o(x^2).$$

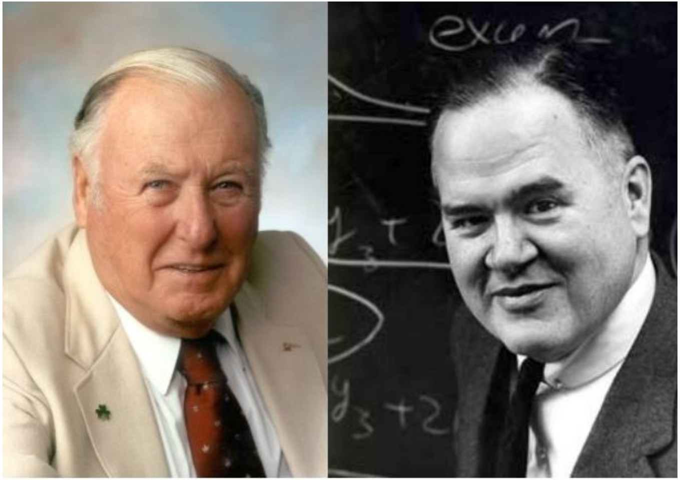
$$\begin{aligned} P_e(t) &= p_0t^0 + p_2t^1 + \cdots + p_{n-2}t^{\frac{n-2}{2}} \\ P_o(t) &= p_1t^0 + p_3t^1 + \cdots + p_{n-1}t^{\frac{n-2}{2}} \end{aligned}$$

also

$$P(-x) = P_e(x^2) - xP_o(x^2).$$

WLOG $n = 2^k$ and evaluate in $\omega^0, \omega^1, \ldots, \omega^{n-1}$.
This is called Discrete Fourier transform (DFT).

Jean-Baptiste Joseph Fourier 1768–1830



James William Cooley (1926-) John Wilder Tukey (1915-2000)

Fast Fourier Transform

FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. If $n = 1$: return (p_0).

Fast Fourier Transform

FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. If $n = 1$: return (p_0).
2. $(e_0, \ldots, e_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_0, p_2, \ldots, p_{n-2}))$
3. $(o_0, \ldots, o_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_1, p_3, \ldots, p_{n-1}))$

Fast Fourier Transform

FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. If $n = 1$: return (p_0).
2. $(e_0, \ldots, e_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_0, p_2, \ldots, p_{n-2}))$
3. $(o_0, \ldots, o_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_1, p_3, \ldots, p_{n-1}))$
4. For $j = 0, \ldots, n/2 - 1$:
5. $\quad y_j \leftarrow e_j + \omega^j \cdot o_j$ (ω^j can be computed incrementally)
6. $\quad y_{j+n/2} \leftarrow e_j - \omega^j \cdot o_j$
7. Return $(y_0, \ldots, y_{n-1})$.

Fast Fourier Transform

FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. If $n = 1$: return (p_0).
2. $(e_0, \ldots, e_{n/2-1}) \leftarrow$ FFT $(n/2, \omega^2, (p_0, p_2, \ldots, p_{n-2}))$
3. $(o_0, \ldots, o_{n/2-1}) \leftarrow$ FFT $(n/2, \omega^2, (p_1, p_3, \ldots, p_{n-1}))$
4. For $j = 0, \ldots, n/2 - 1$:
5. $\quad y_j \leftarrow e_j + \omega^j \cdot o_j$ (ω^j can be computed incrementally)
6. $\quad y_{j+n/2} \leftarrow e_j - \omega^j \cdot o_j$
7. Return $(y_0, \ldots, y_{n-1})$.

Time complexity $T(n) = 2T(n/2) + \Theta(n) = \Theta(n \log n)$.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Step 2 runs on $\Theta(n \log n)$ using FFT. Can we solve step 4 effectively?

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \dots, x_{n-1}$.
2. Compute $(P(x_0), \dots, P(x_{n-1}))$ and $(Q(x_0), \dots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \dots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Step 2 runs on $\Theta(n \log n)$ using FFT. Can we solve step 4 effectively?

Definition (Discrete Fourier Transform (DFT))

Discrete Fourier transform is a mapping $\mathcal{F} : \mathbb{C}^n \to \mathbb{C}^n$ which assigns vector $\vec{x}$ vector $\vec{y}$

$$y_j = \sum_{k=0}^{n-1} x_k \cdot \omega^{jk}.$$

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \dots, x_{n-1}$.
2. Compute $(P(x_0), \dots, P(x_{n-1}))$ and $(Q(x_0), \dots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \dots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Step 2 runs on $\Theta(n \log n)$ using FFT. Can we solve step 4 effectively?

Definition (Discrete Fourier Transform (DFT))

Discrete Fourier transform is a mapping $\mathcal{F} : \mathbb{C}^n \to \mathbb{C}^n$ which assigns vector $\vec{x}$ vector $\vec{y}$

$$y_j = \sum_{k=0}^{n-1} x_k \cdot \omega^{jk}.$$

$\mathcal{F}$ is a linear transformation $\implies$ there exists matrix Ω such that $\mathcal{F}(\vec{x}) = \Omega\vec{x}$.

Inverting Ω

Inverting Ω

$$\Omega_{jk} = \omega^{jk}.$$

$$\omega^{-1} = \overline{\omega}.$$

Inverting Ω

$$\Omega_{jk} = \omega^{jk}.$$

$$\omega^{-1} = \overline{\omega}.$$

Lemma

$\Omega \cdot \overline{\Omega} = n \cdot E.$

Proof.

$$(\Omega \cdot \overline{\Omega})_{jk} = \sum_{\ell=0}^{n-1} \Omega_{j\ell} \cdot \overline{\Omega}_{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega^{\ell k}} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega}^{\ell k}$$

$$= \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot (\omega^{-1})^{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \omega^{-\ell k} = \sum_{\ell=0}^{n-1} \omega^{(j-k)\ell}.$$

Inverting Ω

$$\Omega_{jk} = \omega^{jk}.$$
$$\omega^{-1} = \overline{\omega}.$$

Lemma

$\Omega \cdot \overline{\Omega} = n \cdot E.$

Proof.

$$(\Omega \cdot \overline{\Omega})_{jk} = \sum_{\ell=0}^{n-1} \Omega_{j\ell} \cdot \overline{\Omega}_{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega^{\ell k}} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega}^{\ell k}$$
$$= \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot (\omega^{-1})^{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \omega^{-\ell k} = \sum_{\ell=0}^{n-1} \omega^{(j-k)\ell}.$$

For $j = k$

$$\sum_{\ell=0}^{n-1} \omega^{(j-k)\ell} = \sum_{\ell=0}^{n-1} 1 = n.$$

Inverting Ω

$$\Omega_{jk} = \omega^{jk}.$$
$$\omega^{-1} = \overline{\omega}.$$

Lemma

$\Omega \cdot \overline{\Omega} = n \cdot E.$

Proof.

$$(\Omega \cdot \overline{\Omega})_{jk} = \sum_{\ell=0}^{n-1} \Omega_{j\ell} \cdot \overline{\Omega}_{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega^{\ell k}} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \overline{\omega}^{\ell k}$$
$$= \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot (\omega^{-1})^{\ell k} = \sum_{\ell=0}^{n-1} \omega^{j\ell} \cdot \omega^{-\ell k} = \sum_{\ell=0}^{n-1} \omega^{(j-k)\ell}.$$

For $j = k$

$$\sum_{\ell=0}^{n-1} \omega^{(j-k)\ell} = \sum_{\ell=0}^{n-1} 1 = n.$$

For $j \neq k$:

$$\sum_{\ell=0}^{n-1} \omega^{(j-k)\ell} = \sum_{\ell=0}^{n-1} q^{\ell} = \frac{q^n - 1}{q - 1} = \frac{\omega^{(j-k)n} - 1}{\omega^{j-k} - 1} = 0.$$

□

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Inverse of FFT with ω is also FFT with $\overline{\omega}$.
Step 4 can be solved by the same algorithm.