FAST FOURIER TRANSFORM AND MULTIPLICATION OF POLYNOMIALS

14/04/15

Let f, g be univariate polynomials of degree $\leq n-1$

(*) $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$

$g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_{n-1} x^{n-1}$

HOW FAST CAN WE COMPUTE THE POLYNOMIAL $f \cdot g$?

→ STANDARD APPROACH

$h = f \cdot g = c_0 + c_1 x + \dots + c_{2(n-1)} x^{2(n-1)}$, where

$c_i = \sum_{0 \leq \ell, k : \ell + k = i} a_\ell b_k$ $\Theta(i)$ PRODUCTS AND $\Theta(i)$ SUMS FOR $i \leq n-1$

IN TOTAL $\geq 1 + 2 + \dots + n-1 = \Theta(n^2)$ MULTIPLICATIONS AND ADDITIONS

CAN WE DO BETTER? YES, UNDER REASONABLE ALGEBRAIC ASSUMPTIONS

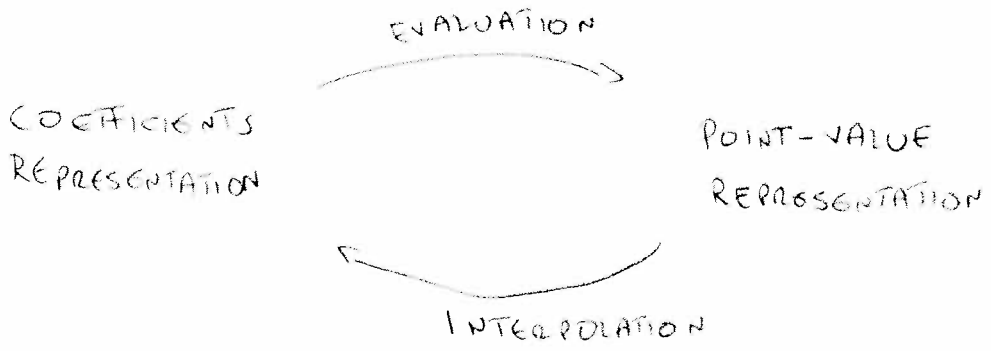
IDEA: INSTEAD OF USING THE COEFFICIENTS REPRESENTATION (*), WE USE THE POINT-VALUE REPRESENTATION

$(x_0, f(x_0)), (x_1, f(x_1)), \dots, (x_{n-1}, f(x_{n-1}))$

THM [YOU SHOULD REMEMBER FROM ALGEBRA COURSES]

GIVEN PAIRS $(u_0, v_0), (u_1, v_1), \dots, (u_n, v_n)$, WITH $u_i, v_i \in$ FIELD F $\forall i$, $u_i \neq u_j$ FOR $i \neq j$

THERE EXISTS EXACTLY ONE POLYNOMIAL OVER F SUCH THAT $f(u_i) = v_i \quad \forall i$.



ALTERNATIVE ALGORITHM FOR MULTIPLICATION OF POLYNOMIALS:

f, g IN COEFFICIENTS REPRESENTATION, OF DEGREE $\leq \frac{n}{2}-1$

$h = f \cdot g$ IN COEFFICIENTS REPRESENTATION

EVALUATION (1)

$(x_0, f(x_0)), (x_1, f(x_1)), \dots (x_n, f(x_n))$

$(x_0, g(x_0)), \dots$

(3) MULTIPLICATION IN P-V REPR.

$(x_0, f(x_0)\cdot g(x_0)), (x_1, f(x_1)g(x_1)) \dots (x_n, f(x_n)g(x_n))$

INTERPOLATION (2)

COMPLEXITY

(1) $\begin{bmatrix} f(x_0) \\ \vdots \\ f(x_n) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_{n-1}^2 \\ & & & & \\ 1 & x_n & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix}$

$n \times n$ INVERTIBLE MATRIX A

$\Theta(n^2)$ MULTIPLICATIONS AND SUMS

(2) $a = A^{-1} \cdot f$ $\Theta(n^2)$ MULTIPLICATIONS AND SUMS

(3) $\Theta(n)$ MULTIPLICATIONS

IDEA OF A FASTER ALGORITHM FOR POLYNOMIAL MULTIPLICATION:

DO (1), (2) FASTER BY CHOOSING $x_0, \dots x_n$ CAREFULLY $\Rightarrow O(n \log n)$ ALGORITHM

IN THE FOLLOWING, WE WILL ASSUME THAT THE COEFFICIENTS OF f BELONG TO A RING R THAT IS COMMUTATIVE WRT MULTIPLICATION

RECALL: RING $(R, +, *)$ → ABELIAN GROUP WRT $+$; HAS "1"; $*$ IS ASSOCIATIVE; $*$ DISTRIBUTES OVER $+$

RINGS COMMUTATIVE WRT MULTIPLICATIONS ARE MORE GENERAL THAN FIELDS

↳ EX. $\mathbb{Z}_N$

EX: $\mathbb{C}$ ←

RINGS HAVE ZERO DIVISORS

DEF. $a \in R$ IS A Z.D. IF $\exists\, b \in R \setminus \{0\}$: $ab = 0$

RECALL $a \in R$ IS INVERTIBLE IF $\exists\, a^{-1} \in R$: $a \cdot a^{-1} = 1$

1. a IS A Z.D. $\Rightarrow$ a IS NOT INVERTIBLE

PF LET $b \neq 0$: $ab = 0$, and suppose by contradiction a^{-1} $\exists$.

Then $0 = a^{-1} \cdot 0 = a^{-1} \cdot ab = b$ ↯ □

SO A FIELD HAS NO ZERO DIVISORS (EVERY ELEMENT IS INVERTIBLE) BUT $\mathbb{Z}_N$ HAS.

E.G. 3 IS A ZERO DIVISOR IN $\mathbb{Z}_{12}$ $[3 \cdot 4 \equiv 0 \bmod 12]$

MOST CRUCIAL FOR US IS:

DEF. $\omega \in R$ IS A PRIMITIVE n-TH ROOT OF UNITY IN R IF:

(i) $\omega^n = 1$
(ii) n IS INVERTIBLE IN R $[n = \overbrace{1+1+\dots+1}^{n}]$
(iii) $\omega^{n/t} - 1$ IS NOT A ZERO DIVISOR IN R $\forall\, t$ PRIMES DIVIDING n

EXAMPLES

* $e^{2\pi i/8}$ IS A PRIMITIVE 8-TH ROOTH IN $\mathbb{C}$

- CLEARLY 8 IS INVERTIBLE IN $\mathbb{C}$ [$\mathbb{C}$ IS A FIELD] $\Rightarrow$ ii) ✓
- $e^{\frac{2\pi i}{8} \cdot 8} = 1 \Rightarrow$ i) ✓
- $e^{\frac{2\pi i}{8} \cdot \frac{1}{2}} - 1$ IS NOT A 0 DIVISOR [$\mathbb{C}$ IS A FIELD] $\Rightarrow$ iii) ✓

* 3 IS A PRIMITIVE 16-TH ROOT OF UNITY IN $\mathbb{Z}_{17}$

- $3^{16} \equiv 1 \mod 17$ [FERMAT'S LITTLE THM.] $\Rightarrow$ i) ✓
- 16 IS INVERTIBLE IN $\mathbb{Z}_{17}$ [$\gcd(16,17)=1$] $\Rightarrow$ ii) ✓
- $3^8 - 1$ IS INVERTIBLE IN $\mathbb{Z}_{17}$ [DO THE MATH]
  $\Rightarrow$ IS NOT A 0 DIVISOR $\Rightarrow$ iii) ✓

FOR A PRIMITIVE n-TH ROOT OF UNITY, w IN R, DEFINE THE VANDERMONDE MATRIX

$$V_w = \begin{pmatrix} w^{0\cdot 0}=1 & w^{0\cdot 1}=1 & w^{0\cdot 2}=1 & \cdots & w^{0\cdot(n-1)}=1 \\ w^{1\cdot 0}=1 & w^{1\cdot 1}=w & w^{1\cdot 2}=w^2 & \cdots & w^{n-1} \\ 1 & w^2 & w^4 & & w^{2(n-1)} \\ \vdots & & & & \\ 1 & w^{n-1} & w^{2(n-1)} & \cdots & w^{(n-1)^2} \end{pmatrix}$$

DEF.

GIVEN R, w AS ABOVE, WE LET THE DISCRETE FOURIER TRANSFORM BE THE MAPPING

$$\text{DFT} \quad R^n \longrightarrow R^n$$

$$a \longrightarrow V_w \cdot a = \begin{bmatrix} f(w^0) \\ f(w^1) \\ \vdots \\ f(w^{n-1}) \end{bmatrix}$$

[DFT COMPUTES THE EVALUATION OF f AT $w^0, w^1, \ldots, w^{n-1}$]

[2] Let $K, m \in \mathbb{N}, c \in R$

$$(1) = (c^K - 1) \sum_{0 \le j \le m-1} c^{jK} = c^{mK} - 1 = (1)$$

PF

$$(1) = c^K - 1 + c^{K+1} - c^K + c^{K+2} - c^{K+1} + \dots + c^{mK} - c^{(m-1)K} = c^{mK} - 1$$

□

[3] Let w be a primitive n-th root of unity. Then, $\forall \ell \in \{1, \dots, n-1\}$

(I) $w^\ell - 1$ IS NOT A ZERO DIVISOR OF R

(II) $\sum_{0 \le j \le n-1} w^{\ell j} = 0$

PF.

(I) Let $\ell \mid n$, $\ell < n \Rightarrow \exists g \in \mathbb{P}: \ell \mid n/g$, let $\ell \cdot m = n/g$. Then

$$\underbrace{w^{n/g} - 1}_{\text{NOT A ZERO DIVISOR}} = \underbrace{(w^\ell - 1) \sum_{0 \le j \le m-1} w^{\ell j}}_{\text{NOT A ZERO DIVISOR}}$$

IF $\ell \nmid n$, Let $g = \gcd(\ell, n) = a \cdot \ell + b \cdot n$ FOR SOME $a, b \in \mathbb{Z}$

Then $w^{a\ell} - 1 = w^{g - bn} - 1 = w^g - 1$ WHICH IS NOT A ZERO DIVISOR (FROM ABOVE)

AS $w^{a\ell} - 1 = (w^\ell - 1) \sum_{0 \le j \le a-1} w^{\ell j} \Rightarrow w^\ell - 1$ IS NOT A ZD

(II)

$$0 = w^n - 1 = w^{\ell n} - 1 = \underbrace{(w^\ell - 1)}_{\text{NOT A ZD}} \underbrace{\sum_{0 \le j \le n-1} w^{j\ell}}_{\Rightarrow\ 0} = 0$$

□

[6] Let w be a primitive n-th root of unity in R. Then w^2 is an $\frac{n}{2}$-th root of unity in R.

PF: exercise

We can now define the algorithm for computing DFT.

IT IS CALLED FAST FOURIER TRANSFORM (FFT)

WLOG n POWER OF 2. SUPPOSE WE HAVE n-TH ROOTS OF UNITY. ω

IDEA: WE WANT TO COMPUTE $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$

OBSERVE: $f(x) = f^{EVEN}(x^2) + x f^{ODD}(x^2)$

$$f^{EVEN}(x) = a_0 + a_2 x + a_4 x^2 + \dots a_n x^{\frac{n}{2}-1}$$

$$f^{ODD}(x) = a_1 + a_3 x + a_5 x^2 + \dots + a_{n-1} x^{\frac{n}{2}-1}$$

} OF DEGREE $\leq \frac{n}{2}-1$

WE HAVE:

$$f(\omega^0) = f^E(\underbrace{\omega^{0\cdot 2}}_{\omega^0}) + f^O(\underbrace{\omega^{0\cdot 2}}_{\omega^0})$$

$$f(\omega) = f^E(\omega^2) + \omega f^O(\omega^2)$$

$$f(\omega^2) = f^E(\omega^4) + \omega^2 f^O(\omega^4)$$

$$f(\omega^{\frac{n}{2}}) = f^E(\omega^{2n}) + \omega^{n/2} f^O(\omega^{2n}) = f^E(\omega^0) - \omega^0 f(\omega^0)$$

ω^0 (BECAUSE $\omega^n = 1$) ω^0

$(\omega^{\frac{n}{2}} - 1)(\omega^{\frac{n}{2}} + 1) = \omega^n - 1 = 0$ BUT $\omega^{\frac{n}{2}} \neq 1$ ('PRIMITIVE')

$\Rightarrow \omega^{\frac{n}{2}} = -1 = -\omega^0$.

SO IN ORDER TO COMPUTE THE VALUES $f(\omega^0), \dots, f(\omega^{n-1})$ I ONLY NEED TO COMPUTE $f^E(\omega^0) \dots f^E(\omega^{\frac{n}{2}-1})$, $f^O(\omega^0), \dots, f^O(\omega^{\frac{n}{2}-1})$

WHICH AGAIN I CAN DO RECURSIVELY, BECAUSE, FROM 3, ω^2 IS AN $(\frac{n}{2})$-TH ROOT OF UNITY IN R.

ALGORITHM

INPUT: $f(x) = [a_0, \ldots, a_{n-1}]$, ω primitive n-TH ROOTH OF UNITY WITH n POWER OF 2.

OUTPUT: $DFT_\omega(a) = [y_0, \ldots, y_{n-1}]$.

- SPLIT f INTO "EVEN" AND "ODD". $f(x) = f^E(x^2) + x f^O(x^2)$
- RECURSIVELY COMPUTE $y^E = DFT_{\omega^2}(f^E)$; $y^O = DFT_{\omega^2}(f^O)$
- SET $h = 1$
- FOR $K = 0$ TO $\frac{n}{2} - 1$ DO:
  - $y_k = y_k^E + h \cdot y_k^O$
  - $y_{k+n/2} = y_k^E - h\, y_k^O$
  - $h = h \cdot \omega$
- return $[y_0, \ldots, y_{n-1}]$

COMPLEXITY:

$$T(n) \leq 2T\left(\frac{n}{2}\right) + \underbrace{cn}_{\text{CONSTANT}} \leq 4T\left(\frac{n}{4}\right) + 2c(n) \leq \ldots$$

$$\leq n \cdot \underbrace{T(2)}_{\text{CONSTANT}} + \log n \cdot c \cdot n = O(n \log n) \quad \square$$

THIS SOLVES THE EVALUATION. HOW ABOUT THE INTERPOLATION?
THIS IS EQUIVALENT TO COMPUTE THE INVERSE OF DFT.

IN FACT,
WE NOW SHOW $\boxed{5}$ $(DFT_\omega)^{-1} = n^{-1}\, DFT_{\omega^{-1}}$

HENCE, COMPUTING THE INVERSE IS AGAIN A DFT
$\rightarrow$ CAN ALSO BE DONE IN TIME $O(n \log n)$ ④

[6] w IS A PRIMITIVE n-TH ROOT OF A RING $\Rightarrow$ w^{-1} "

[PF (i) $(w^{-1})^n = (w^n)^{-1} = 1^{-1} = 1$ ✓
(ii) OBVIOUS
(iii) $(w^{-1})^{\frac{n}{t}} - 1$ ISNOT A 0-DIV FOR $(a-1) = (a^{-1})(-a)$]

[7] R, w, n as always. Then $V_w \cdot V_{w^{-1}} = nI$

[OBS: THIS IMMEDIATELY IMPLIES [5]]

PF

$$(V_w V_{w^{-1}})_{jl} = \sum_{k=0}^{n-1} (V_w)_{jk} (V_{w^{-1}})_{kl} = \sum_{k=0}^{n-1} w^{jk} \cdot w^{-kl}$$

$$= \sum_{k=0}^{n-1} w^{k(j-l)}$$

IF $j = l \Rightarrow (V_w V_{w^{-1}})_{jl} = \sum_{k=0}^{n-1} w^0 = 1 + 1 + \ldots + 1 = n$ ✓

IF $j \neq l \Rightarrow (V_w V_{w^{-1}})_{jl} = \sum_{k=0}^{n-1} w^{kt} = 0$ ✓ [USING [3].(II)] □

IN ORDER TO APPLY FFT, we need R to have n-TH ROOTS OF UNITY, WITH n POWERS OF 2.

Let $M = 2^k + 1$. Let us show that $\mathbb{Z}_M$ HAS THIS PROPERTY.

[8] Let $2^K \mid L$; $K, L \in \mathbb{Z}$. Then $w = 2^{L/2^K} \in \mathbb{Z}_M$ and is a primitive 2^{K+1}-TH root of unity.

PF

(i) $\left(2^{L/2^K}\right)^{2^{K+1}} = 2^{2L} = 2^L \cdot 2^L = (-1)(-1) = 1$ ✓

(ii) $2 \nmid M = 2^L + 1 \Rightarrow \gcd(2^{K+1}, M) = 1 \Rightarrow 2^K \in \mathbb{Z}_M^*$ ✓

(iii) $2^{2L/t} - 1 = 2^L - 1 = -2 = 2^L - 1$ CLEARLY $\gcd(2^L - 1, 2^L + 1) = 1$

($t = 2$ IS THE ONLY PRIME DIVIDING $2K$) (WE OBSERVED ABOVE $2^L = -1$)

$\Rightarrow 2^L - 1$ IS INVERTIBLE IN $\mathbb{Z}_M$

$\Rightarrow$ IT IS NOT A ZD □