7 March 2025

Polynomial Multiplication & Convolution

Plan

* Convolution
* Announcements
* Multiplying Polynomials via FFT

Motivating Example. Sum of Independent RVs.

Roll a die $X \leftarrow \{1,2,3,4,5,6\}$

Roll a second die $Y \leftarrow \{1,2,3,4,5,6\}$

What is the distribution of the sum of dice?

e.g. $\Pr[X+Y=4] = ?$

1 3   2 2   3 1

Motivating Example: Sum of Independent RVs.

X discrete Random Variable over $\{0, 1, 2, \ldots, n\}$

$$\Pr[X = i] = x_i \quad \text{for } i = 0 \ldots n$$

Y discrete RV s.t.

$$\Pr[Y = j] = y_j \quad \text{for } j = 0, 1 \ldots n.$$

For independent X, Y

$$\Pr[X + Y = k] = ?$$

$\Pr[X = i]$ $\qquad x_n \, x_{n-1} \cdots x_2 \, x_1 \, x_0$

$\Pr[Y = j]$ $\qquad y_n \, y_{n-1} \cdots y_2 \, y_1 \, y_0$

$$\Pr[X + Y = k] = \sum_{\substack{i = 1 \ldots n \\ j = 1 \ldots n}} \Pr[X = i \wedge Y = j]$$

$\boxed{\text{s.t. } i + j = k}$

$Pr[X = i]$ $\qquad x_n \, x_{n-1} \cdots x_2 \, x_1 \, x_0$

$Pr[Y = j]$ $\qquad y_n \, y_{n-1} \cdots y_2 \, y_1 \, y_0$

$$Pr[X + Y = k] = \sum_{\substack{i = 1 \ldots n \\ j = 1 \ldots n}} Pr[X = i \wedge Y = j]$$

s.t. $i + j = k$

$\Big\downarrow$ $X \perp\!\!\!\perp Y$ independence

$$= \sum_{i + j = k} Pr[X = i] \cdot Pr[Y = j]$$

$\Pr[X = i]$ $\qquad x_n \, x_{n-1} \cdots x_2 \, x_1 \, x_0$

$\Pr[Y = j]$ $\qquad y_n \, y_{n-1} \cdots y_2 \, y_1 \, y_0$

$$\Pr[X + Y = k] = \sum_{\substack{i = 1 \dots n \\ j = 1 \dots n}} \Pr[X = i \wedge Y = j]$$

s.t. $i + j = k$

$X \perp\!\!\!\perp Y$ independence

$$= \sum_{i+j=k} \Pr[X = i] \cdot \Pr[Y = j]$$

$$= \boxed{\sum_{i+j=k} x_i \cdot y_j}$$

Convolution

Given sequences $p = p_n\, p_{n-1} \cdots p_1\, p_0$

$q = q_n\, q_{n-1} \cdots q_1\, q_0$

Return sequence $c = c_{2n}\, c_{2n-1} \cdots c_2\, c_1\, c_0$

$$c_k = (p * q)_k = \sum_{i+j=k} p_i \cdot q_j$$

Convolution

Given sequences $p = p_n \, p_{n-1} \, \cdots \, p_1 \, p_0$

$q = q_n \, q_{n-1} \, \cdots \, q_1 \, q_0$

Return sequence $c = c_{2n} \, c_{2n-1} \, \cdots \, c_2 \, c_1 \, c_0$

$$c_k = (p * q)_k = \sum_{i+j=k} p_i \cdot q_j$$

Many useful applications!

* Probability Theory
* Signal Processing

Announcements

* HW 4 Ongoing.

* Recitation
  - ↳ More practice w/ flow / reductions

Convolution

Given sequences $p = p_n \, p_{n-1} \, \cdots \, p_1 \, p_0$

$q = q_n \, q_{n-1} \, \cdots \, q_1 \, q_0$

Return sequence $c = c_{2n} \, c_{2n-1} \, \cdots \, c_2 \, c_1 \, c_0$

$$c_k = (p * q)_k = \sum_{i+j=k} p_i \cdot q_j$$

Convolution $\equiv$ $\boxed{\text{Polynomial Multiplication}}$

Polynomial Multiplication

$$p(x) = 3x^2 + 2x - 1$$

$$q(x) = x^3 - x$$

$$p \cdot q(x) = (3x^2 + 2x - 1)(x^3 - x)$$

$$= 3x^5 + 2x^4 - x^3$$

$$- 3x^3 - 2x^2 + x$$

$$3x^5 + 2x^4 - 4x^3 - 2x^2 + x$$

Generalizes Integer Multiplication

$$p(x) = \sum_{i=0}^{n} p_i \cdot x^i \qquad q(x) = \sum_{j=0}^{n} q_j x^j$$

$$p \cdot q(x) = \left(\sum_{i=0}^{n} p_i x^i \right) \left(\sum_{j=0}^{n} q_j x^j \right)$$

$$p(x) = \sum_{i=0}^{n} p_i \cdot x^i \qquad q(x) = \sum_{j=0}^{n} q_j x^j$$

$$p \cdot q(x) = \left(\sum_{i=0}^{n} p_i x^i \right) \left(\sum_{j=0}^{n} q_j x^j \right)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n} p_i q_j \cdot x^{i+j}$$

$$p(x) = \sum_{i=0}^{n} p_i \cdot x^i \qquad q(x) = \sum_{j=0}^{n} q_j \, x^j$$

$$p \cdot q(x) = \left(\sum_{i=0}^{n} p_i \, x^i \right) \left(\sum_{j=0}^{n} q_j \, x^j \right)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n} p_i \, q_j \cdot x^{i+j}$$

$$= \sum_{k=0}^{2n} \left(\sum_{i+j=k} p_i \cdot q_j \right) \cdot x^k$$

$$p(x) = \sum_{i=0}^{n} p_i \cdot x^i \qquad q(x) = \sum_{j=0}^{n} q_j x^j$$

$$p \cdot q(x) = \left(\sum_{i=0}^{n} p_i x^i\right)\left(\sum_{j=0}^{n} q_j x^j\right)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n} p_i q_j \cdot x^{i+j}$$

$$= \sum_{k=0}^{2n} \underbrace{\left(\sum_{i+j=k} p_i \cdot q_j\right)}_{c_k} \cdot x^k$$

Convolution $\equiv$ coefficients of polynomial multiplication

Another Application: Smoothing Signals

* Given n measurements

$$q = q_0\ q_1\ q_2\ \cdots\ q_{n-1}$$

* Return "smoothed" measurements

$$r = r_1\ r_2\ \cdots\ r_{n-1}$$

where $$r_i = \frac{2}{3} q_i + \frac{1}{3} q_{i-1}$$

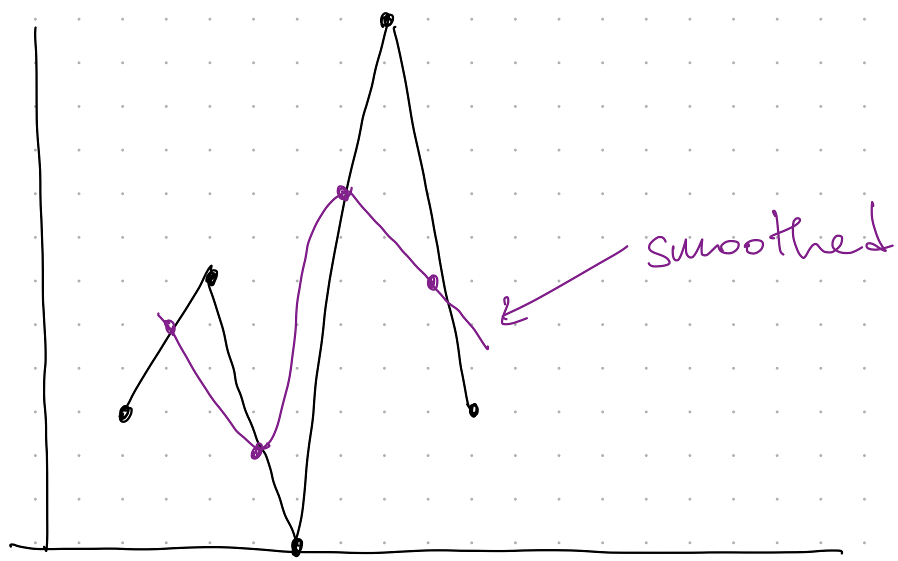
smoothed signal maintains "memory" of last signal

Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$p(x) = 3 + 6x + 12x^3 + 3x^4$

$s(x) = \frac{2}{3} + \frac{1}{3}x$



Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$$p(x) = 3 + 6x + 12x^3 + 3x^4 \qquad s(x) = \frac{2}{3} + \frac{1}{3}x$$

$$\begin{array}{rrrrrrrrrrr}
 & p(x) & 3 & + & 6x & + & 0x^2 & + & 12x^3 & + & 3x^4 \\
* & s(x) & \frac{2}{3} & + & \frac{1}{3}x & & & & & & \\
\hline
 & & 2 & + & 4x & + & 0x^2 & + & 8x^3 & + & 2x^4
\end{array}$$

$(p \cdot s)(x)$

Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$p(x) = 3 + 6x + 12x^3 + 3x^4$ $\qquad s(x) = \frac{2}{3} + \frac{1}{3}x$

$$\begin{array}{lrcccccccccccc}
 & 3 & + & 6x & + & 0x^2 & + & 12x^3 & + & 3x^4 & & \\
p(x) & & & & & & & & & & & \\
* \; s(x) & \frac{2}{3} & + & \frac{1}{3}x & & & & & & & & \\
\hline
 & 2 & + & 4x & + & 0x^2 & + & 8x^3 & + & 2x^4 & & \\
 & & + & x & + & 2x^2 & + & 0x^3 & + & 4x^4 & + & x^5
\end{array}$$

$(p \cdot s)(x)$

Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$$p(x) = 3 + 6x + 12x^3 + 3x^4 \qquad s(x) = \frac{2}{3} + \frac{1}{3}x$$

$$\begin{array}{rrrrrrr}
p(x) & 3 & +\,6x & +\,0x^2 & +\,12x^3 & +\,3x^4 & \\
* \; s(x) & \frac{2}{3} & +\,\frac{1}{3}x & & & & \\
\hline
 & 2 & +\,4x & +\,0x^2 & +\,8x^3 & +\,2x^4 & \\
 & + & x & +\,2x^2 & +\,0x^3 & +\,4x^4 & +\,x^5 \\
\hline
(p \cdot s)(x) & 2 & +\,5x & +\,2x^2 & +\,8x^3 & +\,6x^4 & +\,x^5
\end{array}$$

What is coefficient of x^i?

Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$$p(x) = 3 + 6x + 12x^3 + 3x^4 \qquad s(x) = \frac{2}{3} + \frac{1}{3}x$$

$$\begin{array}{rl}
p(x) & 3 + 6x + 0x^2 + 12x^3 + 3x^4 \\
* \; s(x) & \frac{2}{3} + \frac{1}{3}x \\
\hline
 & 2 + 4x + 0x^2 + 8x^3 + 2x^4 \\
 & + x + 2x^2 + 0x^3 + 4x^4 + x^5 \\
\hline
(p \cdot s)(x) & 2 + 5x + 2x^2 + 8x^3 + 6x^4 + x^5
\end{array}$$

$$6x^4 = \frac{2}{3}(3x^4) + \frac{1}{3}x(12x^3)$$

$$= \left(\frac{2}{3}P_4 + \frac{1}{3}P_3\right)x^4$$

$$= r_4 \cdot x^4$$

Smoothing as Polynomial Multiplication

Signal: $p = 3, 6, 0, 12, 3$

$p(x) = 3 + 6x + 12x^3 + 3x^4$ $\qquad s(x) = \frac{2}{3} + \frac{1}{3}x$

$$
\begin{array}{rrrrrrrrrrrrr}
p(x) & & 3 & + & 6x & + & 0x^2 & + & 12x^3 & + & 3x^4 & & \\
* \; s(x) & & \frac{2}{3} & + & \frac{1}{3}x & & & & & & & & \\
\hline
 & & 2 & + & 4x & + & 0x^2 & + & 8x^3 & + & 2x^4 & & \\
 & & + & & x & + & 2x^2 & + & 0x^3 & + & 4x^4 & + & x^5 \\
\hline
(p \cdot s)(x) & & 2 & + & 5x & + & 2x^2 & + & 8x^3 & + & 6x^4 & + & x^5
\end{array}
$$

$\boxed{r = 5, 2, 8, 6}$

Multiplying Polynomials

* Equivalent to Convolution

* Useful in applications
  - Algebra
  - Probability
  - Signal Processing

* Generalizes Integer Multiplication

Multiplying Polynomials

* Equivalent to Convolution
* Useful in applications
  - Algebra
  - Probability
  - Signal Processing
* Generalizes Integer Multiplication

Question: How quickly can we multiply degree-n polynomials?

$$p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0$$

$$q(x) = q_n x^n + q_{n-1} x^{n-1} + \cdots + q_1 x + q_0$$

Algorithms

$$p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0$$
$$q(x) = q_n x^n + q_{n-1} x^{n-1} + \cdots + q_1 x + q_0$$

Algorithms

* Naive : $\Theta(n^2)$
* Karatsuba : $O(n^{1.59})$
* Better algos?

Representing Polynomials

* Coefficient Representation

Degree-n polynomial $p(x) = \sum_{i=0}^{n} p_i \cdot x^i$

specified uniquely by $p = p_n, p_{n-1}, \ldots, p_1, p_0$

Representing Polynomials

* Coefficient Representation

Degree-n polynomial $\quad p(x) = \sum_{i=0}^{n} p_i \cdot x^i$

specified uniquely by $p = p_n, p_{n-1}, \ldots, p_1, p_0$

* Point-Value Representation

Fundamental Fact. Every Degree-n polynomial is uniquely determined by its evaluation at $n+1$ points.

Representing Polynomials

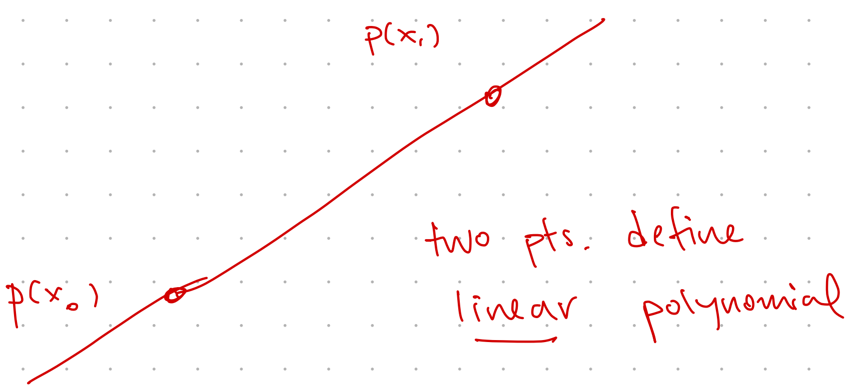
* Coefficient Representation

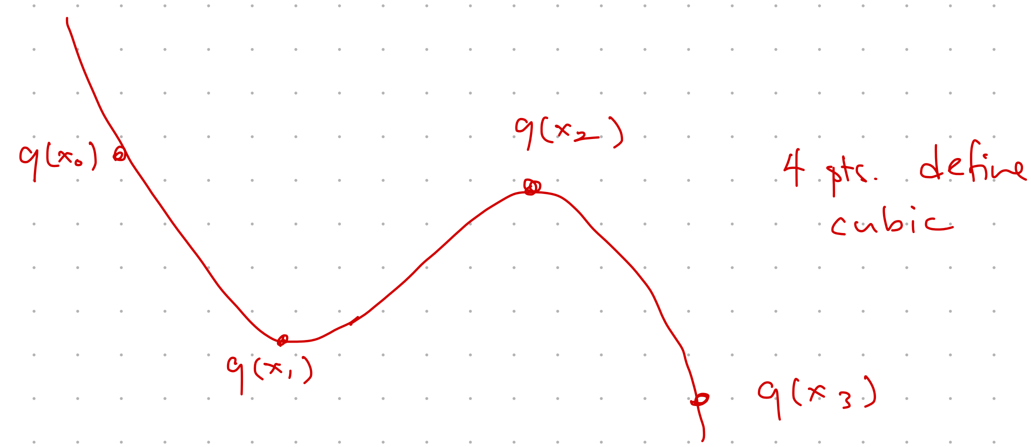
Degree-n polynomial $p(x) = \sum_{i=0}^{n} p_i \cdot x^i$

specified uniquely by $p = p_n, p_{n-1}, \ldots, p_1, p_0$

* Point-Value Representation

<u>Fundamental Fact</u>. Every Degree-n polynomial is uniquely determined by its <u>evaluation</u> at n+1 points.





Key Observation: Multiplication is EASY in Point-Value Representation

	$\hat{p}$	$\hat{q}$	$\widehat{p \cdot q}$
x_0	$p(x_0)$	$q(x_0)$	
x_1	$p(x_1)$	$q(x_1)$	
x_2	$p(x_2)$	$q(x_2)$	
$\vdots$	$\vdots$	$\vdots$	
x_{2n-1}	$p(x_{2n-1})$	$q(x_{2n-1})$	
x_{2n}	$p(x_{2n})$	$q(x_{2n})$	

Key Observation: Multiplication is EASY in Point-Value Representation

	$\hat{p}$	$\hat{q}$	$\widehat{p \cdot q}$
x_0	$p(x_0)$	$q(x_0)$	$p(x_0) \times q(x_0)$
x_1	$p(x_1)$	$q(x_1)$	$p(x_1) \times q(x_1)$
x_2	$p(x_2)$	$q(x_2)$	$p(x_2) \times q(x_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{2n-1}	$p(x_{2n-1})$	$q(x_{2n-1})$	$p(x_{2n-1}) \times q(x_{2n-1})$
x_{2n}	$p(x_{2n})$	$q(x_{2n})$	$p(x_{2n}) \times q(x_{2n})$

Key Observation: Multiplication is EASY in Point-Value Representation

	$\hat{p}$	$\hat{q}$	$\widehat{p \cdot q}$
x_0	$p(x_0)$	$q(x_0)$	$p(x_0) \times q(x_0)$
x_1	$p(x_1)$	$q(x_1)$	$p(x_1) \times q(x_1)$
x_2	$p(x_2)$	$q(x_2)$	$p(x_2) \times q(x_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{2n-1}	$p(x_{2n-1})$	$q(x_{2n-1})$	$p(x_{2n-1}) \times q(x_{2n-1})$
x_{2n}	$p(x_{2n})$	$q(x_{2n})$	$p(x_{2n}) \times q(x_{2n})$

1 multiplication per evaluation point!

$O(n)$ operations

Key Observation: Multiplication is EASY in Point-Value Representation

	$\hat{p}$	$\hat{q}$	$\widehat{p \cdot q}$
x_0	$p(x_0)$	$q(x_0)$	$p(x_0) \times q(x_0)$
x_1	$p(x_1)$	$q(x_1)$	$p(x_1) \times q(x_1)$
x_2	$p(x_2)$	$q(x_2)$	$p(x_2) \times q(x_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{2n-1}	$p(x_{2n-1})$	$q(x_{2n-1})$	$p(x_{2n-1}) \times q(x_{2n-1})$
x_{2n}	$p(x_{2n})$	$q(x_{2n})$	$p(x_{2n}) \times q(x_{2n})$

1 multiplication per evaluation point!

$O(n)$ operations

Requirements

* Evaluation on canonical set of points
  ↳ same set of points for all p, q

Key Observation: Multiplication is EASY in Point-Value Representation

	$\hat{p}$	$\hat{q}$	$\widehat{p \cdot q}$
x_0	$p(x_0)$	$q(x_0)$	$p(x_0) \times q(x_0)$
x_1	$p(x_1)$	$q(x_1)$	$p(x_1) \times q(x_1)$
x_2	$p(x_2)$	$q(x_2)$	$p(x_2) \times q(x_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{2n-1}	$p(x_{2n-1})$	$q(x_{2n-1})$	$p(x_{2n-1}) \times q(x_{2n-1})$
x_{2n}	$p(x_{2n})$	$q(x_{2n})$	$p(x_{2n}) \times q(x_{2n})$

1 multiplication per evaluation point!

$O(n)$ operations

Requirements

* Evaluation on canonical set of points
  ↳ same set of points for all p, q

* Multiplication of $y_i \times z_i$ } Count as $O(1)$

Polynomial Multiplication Road Map

p, q in Coefficient Rep.

$\xrightarrow{\text{polynomial multiplication}}$

$p \cdot q$ in Coefficient Rep

Polynomial Multiplication Road Map

$$\begin{tikzcd}
\boxed{p, q \text{ in Coefficient Rep.}} \arrow[r, dashed, "\text{polynomial multiplication}"] \arrow[d, "\text{Evaluation}"] & \boxed{p \cdot q \text{ in Coefficient Rep}} \\
\boxed{\hat{p}, \hat{q} \text{ in Point-Value Rep}} \arrow[r, "\text{FAST PV Multiply}"] & \boxed{\widehat{p \cdot q} \text{ in Point-Value Rep}} \arrow[u, "\text{Interpolation}"']
\end{tikzcd}$$

$$\begin{array}{lllll}
x_0 & p(x_0) & \times & q(x_0) & = \\
x_1 & p(x_1) & \times & q(x_1) & = \\
\vdots & \vdots & & \vdots & \\
x_{n-1} & p(x_{n-1}) & \times & q(x_{n-1}) & = \\
x_n & p(x_n) & \times & q(x_n) & =
\end{array}$$