21 Feb

Multiplying polynomials and convolution.

Example: 

\[(2x + 1)(4x - 3) = 8x^2 - 2x - 3\]

\[
\begin{array}{c}
2x + 1 \\
4x - 3 \\
\hline
-6x - 3 \\
8x^2 + 4x \\
\hline
8x^2 - 2x - 3
\end{array}
\]

\(\text{Quadratic time } O(\text{degree}^2)\)

\(\text{arithmetic operations}\)

If 

\[A(x) = A_1 x + A_0\]

\[B(x) = B_1 x + B_0\]

and 

\[C(x) = A(x) B(x)\]

then 

\[C(x) = A_1 B_1 x^2 + (A_0 B_1 + A_1 B_0) x + A_0 B_0\]

\[= P_0 x^2 + (P_2 - P_1 - P_0) x + P_0\]

where 

\[P_0 = A_0 B_0\]

\[P_1 = A_1 B_1\]

\[P_2 = (A_0 + A_1) (B_0 + B_1)\]

This is the basis of an \(O(n^{\log_2 3})\) algorithm for multiplying degree \(n\) polynomials, similar to Karatsuba's.
Why multiplying polynomials matters...

1. Basic operation in algebra.

2. Underpinning of integer multiplication (crypto).
   A binary number of \( n \) bits is just a degree \( n-1 \) polynomial evaluated at \( x = 2^i \) with \( \{0,1\} \) coefficients.

3. Polynomials can represent signals (sequences of numbers).
   Multiplication represents convolution.

   **Ex.** Take the sequence:
   
   \[
   0, 2, 4, 3, 4, 1
   \]
   
   and replace every element with the average of the preceding and following ones.

   
   
   \[
   (4x^3 + 8x^2 + 2x + 0)
   \]

   
   
   \[
   \frac{\frac{1}{2}x^2}{\frac{1}{2}} + \frac{1}{x}
   \]

   
   
   \[
   2x^3 + 4x^2 + x + 0
   \]

   
   
   \[
   2x^5 + 4x^4 + x^3 + 0
   \]

   
   
   \[
   2x^9 + 3x^8 + 4x^7 + x + 0
   \]
If \( a_0, a_1, a_2, \ldots \) and 
\( b_0, b_1, b_2, \ldots, b_m \)
are two sequences, their convolution is the sequence \( c_0, c_1, c_2, \ldots, c_{m+n} \)
where
\[
c_k = \sum_{i+j=k} a_i b_j
\]
e.g.
\( c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \).

Often \((a_i)\) is a "signal"/"image" and \((b_j)\) is a "mask"/"weights".

If the sequences \((a_i), (b_j)\) are encoded as polynomials
\[
A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n
\]
\[
B(x) = b_0 + b_1x + \cdots + b_mx^m
\]
then their product \(A \cdot B\) is a polynomial whose coeffs are the convolution of \((a_i)\) and \((b_j)\).

3. Multiplying polynomials encodes summing independent random variables.
Ex. if one rolls two standard dice, what is the probability of every possible sum?

Outcome: 1 2 3 4 5 6

probability: \( \frac{1}{36} \ \frac{1}{18} \ \frac{1}{12} \ \frac{1}{12} \ \frac{1}{12} \ \frac{1}{36} \)

\( \frac{1}{36} (x + x^2 + x^3 + x^4 + x^5 + x^6) \)

"Probability generating function"

\[ \sum_i \Pr(i) x^i \]

If two independent random variables have
prob. gen. func's A and B

\[ A(x) = \sum a_i x^i = \sum \Pr(\text{"Variable A"} = i) \cdot x^i \]

\[ B(x) = \sum b_i x^i = \sum \Pr(\text{"Variable B"} = i) \cdot x^i \]

then \( A(x) \cdot B(x) \) is the PGF of their sum.

Ex. \( \frac{1}{36} x + \frac{2}{36} x^2 + \frac{3}{36} x^3 + \frac{4}{36} x^4 + \frac{3}{36} x^5 + \frac{2}{36} x^6 \)

\[ = \frac{1}{36} x^{11} + \frac{1}{36} x^{12} \]