332:573 – Data Structures & Algorithms

Project Report

Improvements to Polynomial Multiplication Through Fast Fourier Transforms

By David Lambropoulos, Demetrios Lambropoulos

Professor Shantenu Jha
May 6th, 2018

Rutgers University
School of Engineering

Contents

1 Introduction/Motivation

Polynomials are expressions built up of a combination of constants c and symbols called variables. Polynomials with a single indeterminate x can always be written in the form

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 x + a_0$$

where $a_0, ..., a_n$ are constants and x is the indeterminate variable. Polynomials can also be expressed in the following canonical form

$$\sum_{k=0}^{n} a_k x^k$$

Each term in a polynomial is product of some constant called the coefficient of the term and indeterminate raised to a nonnegative integer power n (i.e.$n \in \mathbb{Z}^+$). Polynomials are used in many fields to represent problems or model behavior such as Chemistry, Physics, Economics, Social Scientists, Calculus, Numerical Analysis, etc.

Addition and subtraction of polynomials is easy to implement costing only $O(N)$ time. However, the way polynomials are multiplied is through a method called First, Outer, Inner, Last (FOIL) as can be seen below in Figure 1. The issue with the FOIL method is that it requires too many operations to perform multiplications, especially for large polynomials. Usually real world problems will be modeled with polynomials of 10000+ terms.

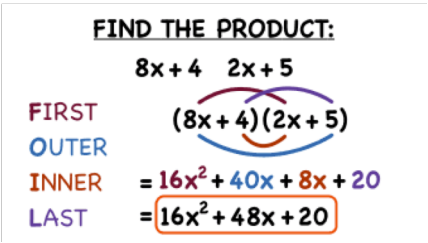


Figure 1: Demonstration of FOIL method

The main scientific motivation behind improving the speed in which we multiple polynomials is that solving large polynomials by hand is tedious and error prone. As discussed previous solving large polynomial multiplications through quadratic algorithms (i.e. FOIL) would cost more time than any person might have. A way that can fix this costly calculation is to implement recursion which uses the divide and conquer method.

2 Algorithms/Theory

Given a polynomial $A(x)$ of length m and a secondary polynomial $B(x)$ of length n then the resultant product would have a length of $m + n - 1$. As mentioned before, a polynomial

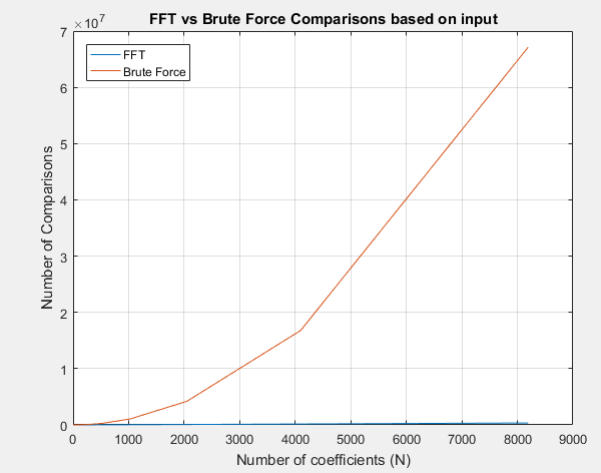
can be represented as a sum of terms consisting of constant coefficients and indeterminate variables as follows:

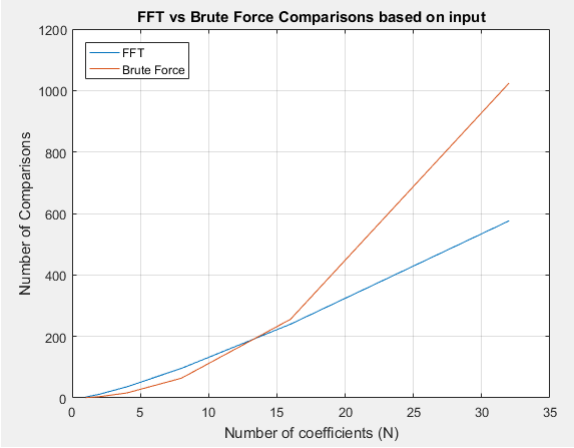
$$A(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1} x^{n-2} + ... + a_1 x + a_0$$

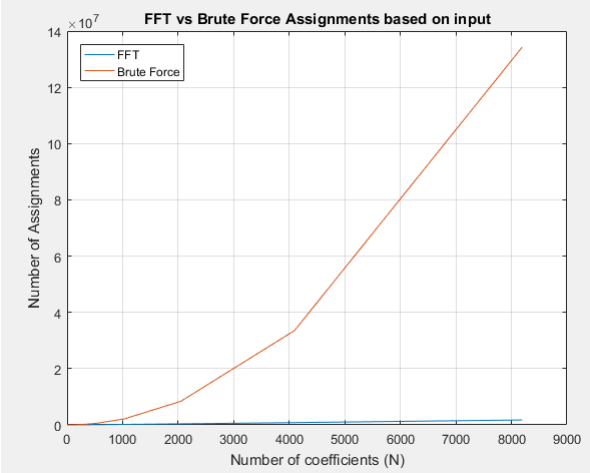
When representing a polynomial in code, we can represent as an array of coefficients in reverse order ($a = [a_0, a_1, ..., a_{n-1}]$). The main advantage to representing this as such allows us to reference coefficients via array indexes.

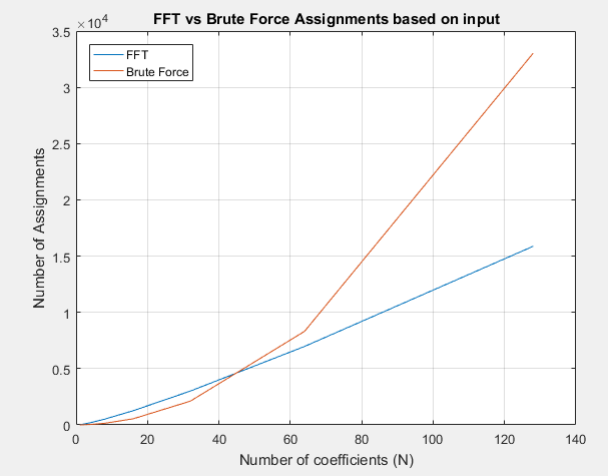
3 Experimental Setup

4 Results and Analysis









5 Discussion

[1]

References

[1] "test," 2017. test.