Multiplying Univariate Polynomials Via Fast Fourier Transforms Over Finite Fields

Stephen D. Fox
Advised by Dr. Robert H. Lewis, Fordham University

May 7, 2011

The Fast Fourier Transform has been known and used for several decades to manipulate polynomials with Real coefficients. Although the coefficients are usually Real in important applications, one needs to use Complex numbers and their roots of unity. Using the Fast Fourier Transform and the Chinese Remainder Theorem, I have implemented a multiplication algorithm for univariate polynomials with coefficients in $\mathbb{Z}$, the integers.

Since the fact that the FFT relies on roots of unity in $\mathbb{C}$ is never used in the algorithm, we can implement the FFT over a finite field using the same mathematical properties of fields needed for the Fast Fouier Transform. We have implemented the Fast Fourier Transform over, $\mathbb{Z}/p$, our choice of finite fields. Using the Chinese Remainder Theorem, this gives rise to an $O(n \lg n)$ algorithm for fast multiplication of univariate polynomials with *integer* coefficients, integers of unlimited number of digits, as is common in computer algebra systems. Results suggest that the FFT over finite fields can provide a significant speedup in polynomial multiplication time over $\mathbb{Z}$.