有限体上での離散フーリエ変換による高速乗算

芝浦工業大学　数理科学研究会
数理科学科 3 年 深谷 徹

平成 26 年 5 月 18 日

1　研究背景

N 桁の多倍長乗算を行う際, 古典的乗算法の計算量は $O(N^2)$ であるが, 高速フーリエ変換を用いると, 計算量が $O(N \log N)$ で済む. 高速フーリエ変換は通常複素数で計算することが多いが, 有限体 $\mathbb{F}_p$ 上でも計算できると知り, 興味が湧いたので研究するに至った.

2　他の多倍長乗算法

2.1　古典的算法

古典的乗算法は, いわゆる掛け算の筆算のことで, 最も基本的な多倍長乗算法である. しかし, N 桁同士の乗算をするときの計算量は $O(N^2)$ である.

2.2　Karatsuba 法

$A = a_1 r + a_0,\ B = b_1 r + b_0$ (r は基数) と表わされる $A,\ B$ の積を求める際, Karatsuba 法では $a_1 b_1 r^2 + (a_1 b_1 + a_0 b_0 - (a_1 - a_0)(b_1 - b_0))r + a_0 b_0$ と計算する. Karatsuba 法を繰り返し適用する事で, 計算量は $O(N^{\log_2 3})$ となる.

3　離散フーリエ変換

N 次の変換元ベクトル $\boldsymbol{x}$, 変換後のベクトル $\boldsymbol{y}$ に対しての離散フーリエ変換は 1 の原始 N 乗根 ζ_N, N 次正方行列 A ($a_{ij} = \zeta_N^{ij},\ 0 \leq i \leq N-1,\ 0 \leq j \leq N-1$), を用いて $\boldsymbol{y} = A\boldsymbol{x}$ のように表せる. また, 逆離散フーリエ変換も N 次正方行列 B ($b_{ij} = \zeta_N^{-ij}$), を用いて $\boldsymbol{x} = \frac{1}{N} B\boldsymbol{y}$ のように表せる.

ある数 $X,\ Y,\ Z$ が $\{x_n\},\ \{y_n\},\ \{z_n\},\ r \geq 2$ ($r \in \mathbb{N}$), $x_n = 0,\ y_n = 0$ $(n \geq N)$ で $X = \sum_{k=0}^{2N-1} x_k r^k,\ Y = \sum_{k=0}^{2N-1} y_k r^k,\ Z = \sum_{k=0}^{2N-1} z_k r^k$ と表されたとする. フーリエ変換した $X,\ Y$ の係数を要素ごとにかけて逆フーリエ変換をすると, 普通に掛け算したのと同じ結果になる.

離散フーリエ変換の規則性を用いて計算量を削減した離散フーリエ変換の計算アルゴリズムを高速フーリエ変換という. 離散フーリエ変換は $O(N^2)$ だが高速フーリエ変換は $O(N \log N)$ になる.

4　有限体でのフーリエ変換

通常, FFT を計算する際 1 の n 原始乗根として, 複素数を用いることが一般的であるが, 有限体上での 1 の原始 n 乗根を用いても離散フーリエ変換, 高速フーリエ変換が出来る. 離散フーリエ変換に使う原始 2^k 乗根を見つける際にかかる計算量を削減する以下の命題を証明した.

> 素数 $p = 2^k n + 1$ ($n,\ k \in \mathbb{N}$) と $\omega \in \mathbb{Z}$ について,
> ω が法 p において原始 2^k 乗根である
> $\Leftrightarrow \omega^{2^{k-1}} \equiv -1 \pmod{p}$

5　FFT アルゴリズムの選択

FFT アルゴリズムの中でも簡単な Cooley-Tukey アルゴリズムを使用していたが, 基数が 2 でない FFT アルゴリズムや six-step FFT アルゴリズム [5] 等の有限体を用いる場合の計算量や, 実行時間等についての比較検討を行う.

参考文献

[1] D.E.KNUTH, 中川圭介訳, KNUTH The Art of Computer Programing=4 準数値算法/算術演算, サイエンス社, 1986.
[2] 高木貞治, 初等整数論講義 第 2 版, 共立出版, 1971.
[3] T.W.KÖRNER, 高橋陽一郎訳, フーリエ解析大全 (上), 朝倉書店, 1996.
[4] T.W.KÖRNER, 高橋陽一郎訳, フーリエ解析大全 (下), 朝倉書店, 1996.
[5] 寒川光, 藤野清次, 長島利夫, 高橋大介, IT Text HPC プログラミング, オーム社, 2009.