日本女子大学紀要　理学部　第12号（2004）

素数を法とする高速フーリエ変換を用いた多倍長整数の乗算

長谷川　暁　子（指導教員　栗原　章）

【序】

さまざまな数値や数式を計算することができるソフトウェアが開発されている。これらを用いた計算は，驚くほどに高速である。私は，なぜこのように速く計算をすることができるのか，ということに興味を持った。そこで，桁数の大きな整数の積を速く計算することを問題にする。

コンピュータを用いて離散フーリエ変換を高速に行うためのアルゴリズムとして，高速フーリエ変換は考案された。1968年に V. Strassen は，高速フーリエ変換の応用として，桁数の大きな整数の積を速く計算することができる新しい方法を見つけた。この V. Strassen の方法を用いて，実際に桁数の大きな整数の積を計算することができるコンピュータプログラムを作ることにする。

【方法】

(1) 桁数の大きな整数同士の和・差・積・商と余りを計算するプログラムを作成する。ここでの積を計算する方法は，一桁一桁を掛けて足すこと（九九と位取り）である。

(2) フーリエ変換を高速フーリエ変換に置き換えた方法を用いて積を計算するプログラムを作成する。これらのフーリエ変換は，有限アーベル群 $\mathbf{Z}/M\mathbf{Z}$ 上（$M=2^l$）で考える。1 の M 乗根を $\zeta=\exp(2\pi\sqrt{-1}/M)$ とする。例えば，$M=4$ とすると，普通のフーリエ変換は（*）式となり，高速フーリエ変換の方法を用いたフーリエ変換は（**）式となる。

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \end{bmatrix} = \begin{bmatrix} \zeta^0 & \zeta^0 & \zeta^0 & \zeta^0 \\ \zeta^0 & \zeta^1 & \zeta^2 & \zeta^3 \\ \zeta^0 & \zeta^2 & \zeta^4 & \zeta^6 \\ \zeta^0 & \zeta^3 & \zeta^6 & \zeta^9 \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \end{bmatrix} \cdots(*),$$

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \zeta^0 & 0 & 0 \\ 1 & \zeta^2 & 0 & 0 \\ 0 & 0 & 1 & \zeta^1 \\ 0 & 0 & 1 & \zeta^3 \end{bmatrix} \begin{bmatrix} 1 & 0 & \zeta^0 & 0 \\ 0 & 1 & 0 & \zeta^0 \\ 1 & 0 & \zeta^2 & 0 \\ 0 & 1 & 0 & \zeta^2 \end{bmatrix} \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \end{bmatrix} \cdots(**)$$

このフーリエ変換で行われる計算は，整数 $\mathbf{Z}$ と ζ による計算である。しかし，ζ は近似値として計算されるため，誤差が生じる。そこで，$\mathbf{Z}[\zeta]$ から $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ への準同型写像が存在すると仮定し，$\mathbf{F}_p$ 内で計算することを考える。このとき，$\mathbf{Z}[\zeta]$ の元 ζ に対応する $\mathbf{F}_p$ の元は，$\mathbf{F}_p^{\times}$ の原始根 g により $g^{(p-1)/M}$ となる。ここで，準同型写像が存在するための必要十分条件は $p\equiv1\pmod{M}$ である。さらに，$\mathbf{F}_p$ 内で計算されたものを整数として復元するための条件も必要となる。これらの条件を満たす素数 p を定め，この p を法とするフーリエ変換を行う。

(3) (1) と (2) で作成した各プログラムでの計算時間を測定し比較する。

【結果と考察】

10進法で約70,000桁同士の積を求める場合，上記の方法を用いて作成したプログラムによる計算時間は，(1) の方法で作成したプログラムによる計算時間の約10倍の速さで計算できることがわかった。また，現在の段階での計算時間は，Mathematica での計算時間の約10倍の計算時間が必要であることもわかった。

【参考文献】

[1] Donald E. Knuth, 準数値算法／算術演算, pp.111-129.
[2] E. Oran Brigham, 高速フーリエ変換, pp.166-191.