第 27 卷 第 3 期 应用数学学报 Vol. 27 No. 3
2004 年 8 月 ACTA MATHEMATICAE APPLICATAE SINICA Aug., 2004

广义 Möbius 变换和算术 Fourier 变换*

高 静
(西安交通大学理学院, 西安 710049)
刘华宁
(西北大学数学系, 西安 710069)

摘 要 离散 Fourier 变换 (DFT) 在数字信号处理等许多领域中占有重要地位. 近年来, 出现一种优于 FFT 的算术 Fourier 变换来计算 DFT. 在广义 Möbius 变换的基础上, 本文采用了一种改进的 AFT 来计算 DFT, 这种方法可以直接提取 DFT 的系数, 且用数论的方法阐明了这一过程, 并展开了进一步的讨论. 这也代表了数论方法应用在计算数学领域的一个新的发展方向.

关键词 广义 Möbius 变换, 算术 Fourier 变换, 离散 Fourier 变换

1 引言

离散 Fourier 变换 (DFT) 在数字信号处理等许多领域中起着非常重要的作用. 但是 DFT 的计算量很大, 所以如果能减少 DFT 的计算量, 将有着深远的意义. Cooley 和 Tukey[1] 的快速 Fourier 变换方法 (FFT) 把 DFT 的计算量从 $O(N^2)$ 降到 $O(N\log N)$, 这大大提高了 DFT 的计算速度, 但 FFT 的程序复杂, 对不同长度的 DFT 其计算公式不一致. 上世纪初, Bruns[2] 提出了算术 Fourier (AFT); Tufts 和 Sadasiv[3] 于 1988 年研究了 AFT 的算法, 计算出了偶周期函数的 Fourier 系数. 它有着比 FFT 很大的优点, 把计算量从 $(N\log N)$ 降到 $O(N)$, 算法简单, 并行性好, 尤其适合 VLSI 设计, 开辟了 DFT 快速计算的新时代. 在 [4] 中, I.S.Reed 等人把 AFT 进行了推广, 使之可以计算周期函数奇、偶部分的系数. 然而这些算法需要把函数延拓为周期函数来计算出中间系数, 且还要从这些系数经过复杂的计算来得到原来的 Fourier 系数, 不能直接提取出 Sine 和 Cosine 的系数.

L. Knockaert[5] 推广了级数的 Möbius 反转公式, 使之可以直接提取 Sine 和 Cosine 的系数. 在 [6] 中, 通过引入周期 q 的既约周期积性算术函数 (RPMA), L. Knockaert 进一步发展了广义 Möbius 变换理论. 而且对于任意 $q\geq 1$, 可以直接得到 Cosine 的系数, 而对某些 q 还可直接得到 Sine 的系数. 这种方法计算简便, 便于并行处理.

在 [6] 的基础上, 本文用数论的方法阐明了这一过程, 并展开了进一步的讨论. 对于这一方法的适用范围, 本文作了分析并给出了完美的解决. 本文对 [6] 中的主要定理给出了另一个简单的证明. 最后, 从应用的角度出发, 本文还给出了算法的主要步骤, 并作了简单的分析.

本文 2002 年 10 月 8 日收到.
* 国家自然科学基金 (10271093 号) 资助项目.

2　广义 Möbius 变换和原根

设 n 为正整数，$f(n), g(n)$ 为定义在整数 $1 \le n \le N$ 上的函数. 根据 [4], 有限级数的 Möbius 反转公式是说：

$$g(n) = \sum_{k=1}^{[N/n]} f(kn), \qquad \text{当且仅当} \qquad f(n) = \sum_{m=1}^{[N/n]} \mu(n) g(mn),$$

其中 $[y]$ 表示 y 的整数部分，$\mu(n)$ 是 Möbius 函数，即就是

$$\mu(n) = \begin{cases} 1, & n = 1; \\ (-1)^r, & n = p_1 \cdots p_r, \quad p_i \text{ 为两两不同的素数}; \\ 0, & \text{其它}. \end{cases}$$

L. Knockaert[5] 推广了级数的 Möbius 反转公式，并证明了下面的定理：

设 $f_1, f_2, f_3, \cdots$ 为实数列，$\alpha(n), \beta(n)$ 为实值算术函数，则

$$S_n = \sum_{k=1}^{\infty} \alpha(k) f_{kn} \qquad \text{及} \qquad f_n = \sum_{k=1}^{\infty} \beta(k) S_{nk}$$

成立的充分必要条件为

$$\sum_{kl=m} \alpha(k)\beta(l) = \delta_{1m} = \begin{cases} 1, & m = 1; \\ 0, & m > 1. \end{cases}$$

在 [6] 中，L. Knockaert 提出了两对广义 Möbius 变换，即就是下面的：

引理 1　当 $q \ge 1$ 时，有

$$S_n = \sum_{(q,k)=1} f_{kn} \qquad \text{及} \qquad f_n = \sum_{(q,k)=1} \mu(k) S_{kn};$$

当 $q > 2$ 且有原根时，则有变换

$$S_n = \sum_{(q,k)=1} (-1)^{\mathrm{ind}\,(k)} f_{kn} \qquad \text{及} \qquad f_n = \sum_{(q,k)=1} \mu(k)(-1)^{\mathrm{ind}\,(k)} S_{kn},$$

其中 $\sum\limits_{(q,k)=1}$ 表示对与 q 互素的 k 求和，$\mathrm{ind}\,(k)$ 为 k 对 q 的原根 g 的指标.

本文将用数论的方法对此展开进一步的分析. 首先，我们列出一些数论中的概念和引理，这些对我们下一步的讨论是必要的.

引理 2　设 Euler 函数 $\phi(n)$ 表示从 1 到 n 之间与 n 互素的整数的数目，则我们有

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

其中 $\prod\limits_{p|n}$ 表示对整数 n 的所有素因数求积.

证　参阅 [7].

设 $m \geq 1$, $(a,m)=1$. 我们把满足 $a^f \equiv 1 \bmod m$ 的最小正整数 f 称为 a 对模 m 的指数. 当 $f=\phi(m)$ 时, 则称 a 是模 m 的原根. 设 g 为模 m 的原根, 则对任意与 m 互素的 a, 存在唯一的整数 k, 满足 $0 \leq k \leq \phi(m)-1$, 使得 $a \equiv g^k (\bmod m)$. 我们把 k 称为 a 对原根 g 模 m 的指标, 记为 $k=\operatorname{ind}(a)$. 显然, $\operatorname{ind}(a)$ 是周期为 m 的函数, 即 $\operatorname{ind}(a)=\operatorname{ind}(a+lm)$.

关于模 m 的原根的存在性, 根据 [7], 我们有下面的:

引理 3 模 m 有原根的充分必要条件是

$$m=1,2,4,p^\alpha,2p^\alpha,$$

其中 p 为奇素数, $\alpha \geq 1$.

综合以上讨论, 我们立刻有

定理 1 m 有原根且 $\phi(m)/2$ 为偶数的充分必要条件为

$$m=p^\alpha,2p^\alpha, \qquad p \equiv 1 \bmod 4;$$

m 有原根且 $\phi(m)/2$ 为奇数的充分必要条件为

$$m=4,p^\alpha,2p^\alpha \qquad p \equiv 3 \bmod 4.$$

其中 p 为奇素数, $\alpha \geq 1$.

下面我们考虑周期为 2π 的实周期函数及 Fourier 级数

$$F(\theta)=\sum_{k=0}^{\infty}\left[f_k\cos(k\theta)+g_k\sin(k\theta)\right],$$

其中 $g_0 \equiv 0$, f_0 已知. 设加权平均值函数

$$S_n=\sum_{r=0}^{q-1}a_r\Big[\frac{1}{n}\sum_{l=0}^{n-1}F\Big(\frac{2\pi}{n}\Big(l+\frac{r}{q}\Big)\Big)\Big],$$

其中 $q \geq 1$ 称为变换的阶, a_r 为实数. L. Knockaert[6] 给出了 S_n 的一个便于应用的等价形式:

引理 4 设 S_n 为上面的和式, 则 S_n 可以表示为

$$S_n=\sum_{r=0}^{q-1}k_r\sum_{k=0}^{\infty}f_{n(qk+r)}+\sum_{r=0}^{q-1}\widetilde{k}_r\sum_{k=0}^{\infty}g_{n(qk+r)},$$

其中, $k_r+i\widetilde{k}_r=\sum_{s=0}^{q-1}a_s e^{2\pi irs/q}$, $r=0,1\cdots,q-1$.

根据上面的讨论, 我们有下面的:

定理 2 对任意 $q>1$, 设

$$a_r^{(1)}=\frac{1}{q}\sum_{(q,s)=1}^{q-1}e^{-2\pi irs/q}. \tag{1}$$

对 $q=p^\alpha,2p^\alpha$ 且 $p \equiv 1 \bmod 4$, 设

$$a_r^{(2)}=\frac{1}{q}\sum_{(q,s)=1}^{q-1}(-1)^{\operatorname{ind}(s)}e^{-2\pi irs/q}. \tag{2}$$

对 $q=4,p^\alpha,2p^\alpha$ 且 $p\equiv 3\bmod 4$ 时，设

$$a_r^{(3)}=\frac{i}{q}\sum_{(q,s)=1}^{q-1}(-1)^{\mathrm{ind}\,(s)}e^{-2\pi irs/q}. \tag{3}$$

再设 $S_n^{(1)},S_n^{(2)},S_n^{(3)}$ 为引理 4 中相应于 $a_r^{(1)},a_r^{(2)},a_r^{(3)}$ 的和式，则我们有

$$f_n=\sum_{(q,k)=1}\mu(k)S_{kn}^{(1)}, \tag{4}$$

$$f_n=\sum_{(q,k)=1}\mu(k)(-1)^{\mathrm{ind}\,(k)}S_{kn}^{(2)}, \tag{5}$$

以及

$$g_n=\sum_{(q,k)=1}\mu(k)(-1)^{\mathrm{ind}\,(k)}S_{kn}^{(3)}. \tag{6}$$

证　我们只从式 (2) 出发来证明式 (5). 类似地，我们可以证明其它等式.

当 $q=p^\alpha$ 或 $2p^\alpha$ 且 $p\equiv 1\bmod 4$ 时，由定理 1 我们知道 q 有原根且 $\phi(q)/2$ 为偶数. 在引理 4 中设 $a_r=\frac{1}{q}\sum\limits_{(q,s)=1}^{q-1}(-1)^{\mathrm{ind}\,(s)}e^{-2\pi irs/q}$，$\tilde{k_r}\equiv 0$，则

$$\begin{aligned}k_r=&\sum_{s=0}^{q-1}\frac{1}{q}\sum_{(l,q)=1}^{q-1}(-1)^{\mathrm{ind}\,(l)}e^{2\pi i(r-l)s/q}\\=&\frac{1}{q}\sum_{(l,q)=1}^{q-1}(-1)^{\mathrm{ind}\,(l)}\sum_{s=0}^{q-1}e^{2\pi i(r-l)s/q}.\end{aligned}$$

注意到

$$\frac{1}{q}\sum_{s=0}^{q-1}e^{2\pi ims/q}=\begin{cases}1, & \text{如果 } q \text{ 整除 m;}\\ 0, & \text{如果 } q \text{ 不整除 } m.\end{cases}$$

及 $(l,q)=1$，$0\le r,\ l\le(q-1)$，则只有当 $r=l$ 时，$\sum\limits_{s=0}^{q-1}e^{2\pi ims/q}=q$. 故

$$k_r=\begin{cases}(-1)^{\mathrm{ind}\,(r)}, & (q,r)=1;\\ 0, & (q,r)\ne 1.\end{cases}$$

相应地，

$$S_n=\sum_{r=0}^{q-1}k_r\sum_{k=0}^{\infty}f_{n(qk+r)}=\sum_{(r,q)=1}^{q-1}(-1)^{\mathrm{ind}\,(r)}\sum_{k=0}^{\infty}f_{n(qk+r)}.$$

令 $qk+r=t$，注意到 $\mathrm{ind}\,(k)$ 是周期为 q 的函数，从而

$$S_n=\sum_{(t,q)=1}^{\infty}(-1)^{\mathrm{ind}\,(qk+r)}f_{nt}=\sum_{(t,q)=1}^{\infty}(-1)^{\mathrm{ind}\,(t)}f_{nt}.$$

根据引理 1, 可得

$$f_n = \sum_{(q,k)=1} \mu(k)(-1)^{\mathrm{ind}\,(k)} S_{kn}.$$

于是完成了定理的证明.

3 算法及结论

这节我们从应用的角度列出算法步骤如下:

1) 输入采样信号 $F(\theta)$, 给定变换的阶 q.

2) 计算 $a_r^{(1)} = \frac{1}{q} \sum\limits_{(q,s)=1}^{q-1} e^{-2\pi irs/q}$ 及加权平均值函数 $S_n^{(1)} = \sum\limits_{r=0}^{q-1} a_r^{(1)} \big[\frac{1}{n} \sum\limits_{l=0}^{n-1} F\big(\frac{2\pi}{n}\big(l + \frac{r}{q}\big)\big)\big]$.

3) 计算 Cosine 的系数 $f_n = \sum\limits_{(q,k)=1} \mu(k) S_{kn}^{(1)}$.

4) 如果 $q = 4, p^\alpha, 2p^\alpha$ 且 $p \equiv 3 \bmod 4$, 则继续下面的步骤.

5) 计算 $a_r^{(3)} = \frac{i}{q} \sum\limits_{(q,s)=1}^{q-1} (-1)^{\mathrm{ind}\,(s)} e^{-2\pi irs/q}$ 及函数 $S_n^{(3)} = \sum\limits_{r=0}^{q-1} a_r^{(3)} \big[\frac{1}{n} \sum\limits_{l=0}^{n-1} F\big(\frac{2\pi}{n}\big(l + \frac{r}{q}\big)\big)\big]$.

6) 计算 Sine 的系数 $g_n = \sum\limits_{(q,k)=1} \mu(k)(-1)^{\mathrm{ind}\,(k)} S_{kn}^{(3)}$.

从上面的步骤我们可以看出, 算法思想简单, 便于并行处理. 本算法对于任何 q 均可直接求出 Cosine 的系数 $f(n)$; 更进一步, 若 q 满足某种条件, 还可直接求出 Sine 的系数. 这是一个将数论方法应用到计算数学领域中的典型, 代表着当今多学科交叉渗透的发展趋势.

致谢 本文写作过程中, 得到了张文鹏教授的悉心指导, 作者在此表示衷心的感谢!

参 考 文 献

1 Cooley J W, Tukey J W. An Algorithm for the Machine Calculation of Complex Fourier Series. *Math. Computat.*, 1965, 19: 297–301

2 Bruns H. Grundlinien des Wissenschaftlichichnen Rechnens. Leipzig: B. G. Teubner Verlag, 1903

3 Tufts D W, Sadasiv G. The Arithmetic Fourier Transform. *IEEE ASSP Mag.*, 1988, 5(1): 13–17

4 Reed I S, Tufts D W, Yu Xiao, et al. Fourier Analysis and signal Processing by Use of Möbius Inversion Formula. *IEEE Trans. Acoust. Speech Singal Processing*, 1990, 38(3): 458–470

5 Knockaert L. A Generalized Möbius Transform and Arithmetic Fourier Transform. *IEEE Trans. Signal Processing*, 1994, 42(11): 2967–2971

6 Knockaert L. A Generalized Möbius Transform, Arithmetic Fourier Transform and Primitive Roots. *IEEE Trans. Signal Processing*, 1996, 44(5): 1307–1310

7 Apostol T M. Introduction to Analytic Number Theory. New York: Springer-Verlag, 1976

GENERALIZED MÖBIUS TRANSFORM AND ARITHMETIC FOURIER TRANSFORM

GAO JING

(*School of Sciences, Xi'an Jiaotong University, Xi'an* 710049)

LIU HUANING

(*Department of Mathematics, Northwest University, Xi'an* 710069)

Abstract The Discrete Fourier Transform (DFT) plays an important role in digital signal processing and many other fields. Recently a method called the Arithmetic Fourier Transform (AFT) that is better than FFT is used to compute DFT. In this paper, an improved AFT based on generalized Möbius inverse formula is used to compute DFT. This new method can extract directly the Fourier coefficients of DFT. We develop this process with the number theory method and extend the further discussion. This also leads to a new direction that Number Theory method is applied into Computation Methematics.

Key words Generalized Möbius transform, arithmetic fourier transform, discrete fourier transform