有限 Fourier 分析

1 $Z(N)$ 上的 Fourier 分析

我们用 Z 表示整数群。假定 N 是一个正整数。一个复数 z 被称为 N **阶单位根** 倘若 $z^N = 1$. 那么，所有 N 阶单位根组成的集合是

$$Z(N) := \{1, e^{2\pi i/N}, e^{2\pi i 2/N}, \ldots, e^{2\pi i(N-1)/N}\}.$$

因此, 如果 $\zeta = e^{2\pi i/N}$, 那么 ζ^k 能产生所有的 N 阶单位根。容易验证，$Z(N)$ 是一个 Abelian 群，其运算为复数的乘法。一个简单的观察是群 $Z(N)$ 同构于 Z/NZ 。我们用 W 和 V 分别表示定义在 Z/NZ 和 $Z(N)$ 上的复值函数空间。

我们现在考察定义在 $Z(N)$ 上的复值函数空间 V. 对于 $f, g \in V$, 我们定义其内积为

$$(f, g) = \frac{1}{N} \sum_{k=0}^{N-1} f(k)\overline{g(k)}.$$

我们首先考察 N 个函数 $e_0, \ldots, e_{N-1}$

$$e_\ell(k) = \zeta^{\ell k} = e^{2\pi i \ell k/N}$$

引理 1.1 函数族 $\{e_0, \ldots, e_{N-1}\}$ 是正交的。事实上,

$$(e_\ell, e_\ell) = 1, \quad (e_m, e_\ell) = 0, m \neq \ell.$$

那么，容易看出 $e_0, \ldots, e_{N-1}$ 是 V 的一个基底。对于 $f \in V$ ，我们定义 f 的第 n 个 Fourier 系数为

$$a_n = (f, e_n) = \frac{1}{N} \sum_{j=0}^{N-1} f(j)e^{-2\pi ijn/N}.$$

那么，我们有

定理 1 如果 f 是 $Z(N)$ 上的一个函数，那么

$$f(k) = \sum_{n=0}^{N-1} a_n e^{2\pi ink/N}.$$

此外,

$$\sum_{n=0}^{N-1} |a_n|^2 \;=\; \frac{1}{N}\sum_{k=0}^{N-1} |f(k)|^2.$$

2 快速 Fourier 变换

假定 N 是固定的。我们设置 $\omega_N := e^{-2\pi i/N}$ 。假设我们知道 $f(0), \ldots, f(N-1)$ 。如果我们用 $a_k^N(f)$ 表示 f 的第 k 个 Fourier 系数。那么，根据定义

$$a_k^N(f) \;=\; \frac{1}{N}\sum_{r=0}^{N-1} f(r)\omega_N^{kr}.$$

那么, 计算所有的 Fourier 系数, 即 $a_k^N(f), k = 0, \ldots, N-1$, 所需的运算次数 $\leq 2N^2 + N$ 。那么，我们能降低这个运算次数吗？

定理 2 假设 $\omega_N = e^{-2\pi i/N}$ 和 $N = 2^n$ 。可以用至多

$$4 \cdot 2^n n = 4N\log_2(N) = O(N\log N)$$

次运算，计算一个函数在 $Z(N)$ 上的 *Fourier* 系数。

我们用 $T(M)$ 标记计算在 $Z(M)$ 上函数 f 的 Fourier 系数所需的最小运算次数。那么，下面引理是证明上述定理的关键步骤。

引理 2.1

$$T(2M) \;\leq\; 2T(M) + 8M.$$

基于上面的引理，我们现在可以证明定理 2 。首先容易验证当 $n = 1$ 时定理成立。假定定理成立当 $N = 2^{n-1}$ ，那么 $T(N) \leq 4 \cdot 2^{n-1}(n-1)$ 。那么，根据上述引理,

$$T(2N) \leq 2 \cdot 4 \cdot 2^{n-1}(n-1) + 8 \cdot 2^{n-1} = 4 \cdot 2^n n.$$

3 有限 Abelian 群上的 Fourier 分析

Abelian **群** 是一个集合 G 及其上的一个二元运算 $(a, b) \mapsto a \cdot b$ ，满足下面的条件：

(i) 分配律：对于所有的 $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ 。

(ii) 单位元：存在一个元素 $u \in G$(通常写作 1 或 0) ，使得 $a \cdot u = u \cdot a = a$ 对所有的 $a \in G$ 成立。

(iii) 逆元：对每一个 $a \in G$ ，存在一个元素 $a^{-1} \in G$ ，使得 $a \cdot a^{-1} = a^{-1} \cdot a = u$ 。

(iv) 交换率：对于 $a, b \in G$ ，我们有 $a \cdot b = b \cdot a$ 。

Abelian 群的例子：

1. 实数集合与通常的加法运算，单位元为 0 ， x 的逆元为 $-x$ 。所有的正实数集合和标准的乘法，单位元为 1 ， x 的逆元为 $1/x$ 。

2. 所有整数的集合 Z 与通常的加法运算。但是 $Z \setminus \{0\}$ 在乘法运算下不是一个 *Abelian* 群。

3.$Z(N)$ 与通常的复数乘法运算。

4. $Z^*(q)$ 的元素为有乘法逆元的整数 (在模 q 的意义下)。其群运算为模 q 的乘法。

我们说两个 Abelian 群 G 和 H 是 **同态** 的，如果存在一个映射 $f : G \to H$ 且满足性质：

$$f(a \cdot b) \ = \ f(a) \cdot f(b).$$

如果存在一个从 G 到 H 的双射同态，那么我们说 G 和 H 是 **同构** 的，记作 $G \approx H$ 。等价的说， G 和 H 是同构的，如果存在另外一个同态映射 $\tilde{f} : H \to G$ 使得对所有的 $a \in G$ 和 $b \in H$

$$(\tilde{f} \circ f)(a) \ = \ a, \qquad (f \circ \tilde{f})(b) \ = \ b.$$

下面，我们主要关注有限 Abelian 群，我们用 $|G|$ 表示群 G 内元素数目。称 $|G|$ 为群 G 的阶。例如， $Z(N)$ 的阶为 N 。假设 G_1, G_2 是两个有限 Abelian 群，它们的 **直积**$G_1 \times G_2$ 是有如下元素组成的群 $(g_1, g_2), g_1 \in G_1, g_2 \in G_2$ 。其运算定义为

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2').$$

那么，直积的定义能够推广到多个情形：

$$G_1 \times G_2 \times \cdots \times G_n.$$

有限 Abelian 群的分类定理说：

任一个有限 Abelian **群同构于一个形式为** $Z(N_1) \times Z(N_2) \times \cdots \times Z(N_n)$ **的群**。

我们下面简单的介绍一个有限 Abelian 群。假定 q 是一个正整数。明显的，我们能在

$$Z(q) := \{0, 1, \ldots, q-1\}$$

中定义乘法。一个整数 $n \in Z(q)$ 被称为 **unit** 如果存在一个整数 $m \in Z(q)$ 使得

$$nm \equiv 1 \mod q.$$

我们将 $Z(q)$ 中所有的 units 组成的集合标记为 $Z^*(q)$ 。明显的， $Z^*(q)$ 在模 q 乘法运算下是一个 Abelian 群。

例：在 $Z(4) = \{0, 1, 2, 3\}$ 中的 units 是

$$Z^*(4) = \{1, 3\}.$$

$Z(5) = \{0, 1, 2, 3, 4\}$ 中的 units 是

$$Z^*(5) = \{1, 2, 3, 4\}.$$

$Z(8) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ 中的 units 是

$$Z^*(8) = \{1, 3, 5, 7\}.$$

4 特征标

令 G 是一个有限 Abelian 群， S^1 是复平面上的单位圆。群 G 上的特征标是一个复值函数 $e : G \to S^1$ 满足下面的条件：对所有 $a, b \in G$

$$e(a \cdot b) \ = \ e(a)e(b).$$

一个平凡的特征标是 $e(a) = 1$ 对所有的 $a \in G$ 。如果 G 是一个有限 Abelian 群，我们用 $\hat{G}$ 表示 G 上的所有特征标。事实上，这个集合继承了 Abelian 群的结构。

引理 4.1 在下面的运算下：

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a), \ \forall a \in G.$$

集合 $\hat{G}$ 是一个 *Abelian* 群.

我们称 $\hat{G}$ 是 G 的 **对偶群**.

例：如果 $G = Z(N)$,G 的所有的特征标为如下形式：

$$e_\ell(k) = e^{2\pi i \ell k/N}, 0 \leq \ell \leq N - 1.$$

此外， $Z(\hat{N})$ 与 $Z(N)$ 同构。

例：R 上的特征标为如下形式

$$e_\xi(x) = e^{2\pi i\xi x}, \xi \in R.$$

例：因为 $\exp : R \to R_+$ 是一个同构映射。那么，我们从上面例子可导出 R_+ 上的特征标是 $e_\xi(x) = x^{2\pi i\xi} = e^{2\pi i\xi \log x}$.

引理 4.2 令 G 是一个有限 *Abelian* 群， $e : G \to C \setminus \{0\}$ 是一个乘法函数，即 $e(a \cdot b) = e(a) \cdot e(b)$ 对所有的 $a, b \in G$ 。那么， e 是一个特征标。

5 正交关联

令 V 表示定义在有限 Agelian 群 G 上的复值函数空间。注意到 V 的维数是 $|G|$ 。我们定义 V 上的 Hermitian 内积为

$$(f, g) \ = \ \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}, \quad f, g \in V.$$

定理 3 G 的特征标形成了一个正交族。

这个定理的证明需要借助下面的引理：

引理 5.1 如果 e 是群 G 的非平凡特征标，那么

$$\sum_{a \in G} e(a) \ = \ 0.$$

由上述定理我们看到,不同的特征标是线性独立的。因为 V 的维数是 $|G|$,我们看到 $|\hat{G}| \leq |G|$ 。下面我们要做的事情是显示 $|\hat{G}| = |G|$ 。

定理 4 有限 *Abelian* 群 G 的特征标形成了 G 上函数空间的一个基底。

6 Plancherel 公式

假定 G 是一个有限 Abelian 群， f 是在 G 上的一个函数， e 是 G 的一个特征标。那么，我们定义 f 相对于 e 的 Fourier 系数为

$$\hat{f}(e) = (f, e) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)},$$

那么 f 的 Fourier 级数为

$$f \sim \sum_{e \in \hat{G}} \hat{f}(e)e.$$

因为特征标形成了一个基，我们有

$$f = \sum_{e \in \hat{G}} c_e e$$

对某些常数 c_e 。通过特征标的正交性，我们有

$$(f, e) = c_e.$$

因此， f 确实等于它的 Fourier 级数。也就是

$$f = \sum_{e \in \hat{G}} \hat{f}(e)e.$$

那么，我们总结我们的结果如下：

定理 5 令 G 是一个有限 *Abelian* 群。 G 的特征标形成了 V 的一个正交基底。特别的，G 上的任意函数 f 等于它的 *Fourier* 级数

$$f = \sum_{e \in \hat{G}} \hat{f}(e)e.$$

最后，我们介绍有限 Abelian 群上的 Parseval-Plancherel 公式：

定理 6 如果 f 是 G 上的一个函数，那么

$$\|f\|^2 = \sum_{e \in \hat{G}} |\hat{f}(e)|^2.$$