一类积性函数的性质与其在计数问题中的应用

北京十一学校　苏阳

2019 年 4 月

关键词：莫比乌斯函数、欧拉函数、狄利克雷卷积、莫比乌斯反演、杜教筛

摘要

积性函数是一类有着特殊性质的函数，可以用于解决许多计数问题．这篇文章含有有关积性函数一般性质，莫比乌斯函数、欧拉函数的性质，狄利克雷卷积，莫比乌斯反演，以及关于使用杜教筛算法计算积性函数前缀和的数学推导的内容和部分证明．这是一篇有关数学的研学报告，所以本文不会在算法层面做过多的展开，而是主要侧重于数学方面的推导和证明．

1 积性函数

1.1 定义与基本性质

数论函数是指定义域在正整数域上，而值域在复数域上的函数，即是：$\mathbf{f} : \mathbb{Z}^+ \to \mathbb{C}$．本文中所涉及的数论函数值域都在整数域上．

积性函数是一种特殊的数论函数，他们满足对于任意互质[1]的一对数p, q，有$\mathbf{f}(p) \cdot \mathbf{f}(q) = \mathbf{f}(pq)$，即他们的函数值乘起来等于他们乘起来的函数值．特别地，如果对于任意不互质两数上面的条件也成立，则称这个函数为**完全积性函数**．

对于一个积性函数$\mathbf{f}$，它在1处的取值一定为1，即$\mathbf{f}(1) = 1$，除非它的所有函数值都是零．我们在下文中不考虑$\mathbf{f}(n) \equiv 0$的情况．

我们定义两个积性函数的加法为逐项相加：

$$(\mathbf{f} + \mathbf{g})(n) = \mathbf{f}(n) + \mathbf{g}(n)$$

我们还定义积性函数的数乘：

$$(x\mathbf{f})(n) = x \times \mathbf{f}(n)$$

1.2 常用的积性函数

以下是常用的一些积性函数：

- $\mu(n)$，**莫比乌斯函数**．它的定义比较复杂，留到狄利克雷卷积后．
- $\varphi(n) = \sum_{i=1}^{n} [\gcd(i, n) = 1]$，**欧拉函数**，即在比不大于这个数的与他互质的数的个数．
- $\mathbf{d}(n) = \sum_{i|n} 1 = \sum_{i=1}^{n} [i|n]$，**约数个数**．
- $\sigma(n) = \sum_{i|n} i = \sum_{i=1}^{n} [i|n] \cdot i$，**约数和**，即这个数的各个约数之和．

以下是一些在证明和推导中常用的完全积性函数：

- $\epsilon(n) = [n = 1]$，**元函数**，只在n为1时为1，其他时候都为0．

[1]我们对两数p, q互质的定义为$\gcd(p, q) = 1$，所以我们称1和其他所有数都互质．

- $\mathbf{1}(n) = 1$，**恒等函数**，他的值永远等于1.
- $\mathbf{id}(n) = n$，**单位函数**.

关于积性函数的性质与证明，我们留到狄利克雷卷积后叙述.

2 狄利克雷卷积和积性函数性质

2.1 狄利克雷卷积

定义两个数论函数**f**和**g**的**狄利克雷卷积**$*$：

$$(\mathbf{f} * \mathbf{g})(n) = \sum_{d|n} \mathbf{f}(d) \times \mathbf{g}(\frac{n}{d})$$

这相当于枚举n的每一个约数，把相应的一对因数分别带进去求值乘起来，然后再都加起来.

狄利克雷卷积满足以下运算规则：

- **交换律**：$\mathbf{f} * \mathbf{g} = \mathbf{g} * \mathbf{f}$
- **结合律**：$(\mathbf{f} * \mathbf{g}) * \mathbf{h} = \mathbf{f} * (\mathbf{g} * \mathbf{h})$，简略证明：

$$\sum_{(i\times j)\times k=n} (\mathbf{f}(i) \times \mathbf{g}(j)) \times \mathbf{h}(k) = \sum_{i\times(j\times k)=n} \mathbf{f}(i) \times (\mathbf{g}(j) \times \mathbf{h}(k))$$

因而，我们不再区分$(\mathbf{f} * \mathbf{g}) * \mathbf{h}$和$\mathbf{f} * (\mathbf{g} * \mathbf{h})$，并直接写作$\mathbf{f} * \mathbf{g} * \mathbf{h}$.

- **数值结合律**：$(x\mathbf{f}) * \mathbf{g} = x(\mathbf{f} * \mathbf{g})$
- **单位元**：$\epsilon * \mathbf{f} = f$，其中$\epsilon(n) = [n = 1]$为上面定义的元函数.
- **逆元**：对于每一个$\mathbf{f}(1) \neq 0$的函数**f**，都有一个函数**g**使得$\mathbf{f} * \mathbf{g} = \epsilon$.

我们有了一个函数**f**，如何得到它的逆元**g**呢？简单的算术可以得出：

$$\mathbf{g}(n) = \frac{1}{\mathbf{f}(1)} \left([n = 1] - \sum_{i|n, i\neq 1} \mathbf{f}(i) \times \mathbf{g}\left(\frac{n}{i}\right) \right)$$

证明：

$$\begin{aligned}(\mathbf{f}*\mathbf{g})(n) &= \sum_{i|n}\mathbf{f}(i)\times\mathbf{g}(\frac{n}{i})\\ &= \mathbf{f}(1)\mathbf{g}(n)+\sum_{i|n,d\neq 1}\mathbf{f}(i)\mathbf{g}(\frac{n}{i})\\ &= [n=1]-\sum_{i|n,i\neq 1}\mathbf{f}(i)\times\mathbf{g}\left(\frac{n}{i}\right)+\sum_{i|n,i\neq 1}\mathbf{f}(i)\times\mathbf{g}\left(\frac{n}{i}\right)\\ &= [n=1]=\epsilon(n)\end{aligned}$$ □

有一个重要结论：**两个积性函数的狄利克雷卷积还是积性函数.**

证明：考虑到若$n\perp m$，则对于任意的a和b使得$a|n,b|m$，都会有$a\perp b$并且$(d=ab)|nm$. 于是若$n\perp m$，我们就有：

$$\begin{aligned}(\mathbf{f}*\mathbf{g})(nm) &= \sum_{d|nm}\mathbf{f}(d)\times\mathbf{g}\left(\frac{nm}{d}\right)\\ &= \sum_{a|n}\sum_{b|m}\mathbf{f}(ab)\times\mathbf{g}\left(\frac{nm}{ab}\right)\\ &= \sum_{a|n}\sum_{b|m}\mathbf{f}(a)\times\mathbf{f}(b)\times\mathbf{g}(\frac{n}{a})\times\mathbf{g}(\frac{m}{b})\\ &= \left(\sum_{a|n}\mathbf{f}(a)\mathbf{g}\left(\frac{n}{a}\right)\right)\times\left(\sum_{b|m}\mathbf{f}(b)\mathbf{g}\left(\frac{m}{b}\right)\right)\\ &= (\mathbf{f}*\mathbf{g})(n)\times(\mathbf{f}*\mathbf{g})(m)\end{aligned}$$ □

还有一个重要结论：**一个积性函数的逆元还是积性函数.**

证明：令积性函数$\mathbf{f}$的逆元为$\mathbf{g}$，考虑数学归纳法：

- $\mathbf{g}(1)$显然为1.
- 假设当$nm>1$，且对于任意$n'm'<nm$，命题都成立时，有：

$$\begin{aligned}\mathbf{g}(nm) &= -\sum_{d|nm,d\neq 1}\mathbf{f}(i)\times\mathbf{g}\left(\frac{nm}{d}\right)\\ &= -\sum_{a|n,b|m,ab\neq 1}\mathbf{f}(ab)\times\mathbf{g}\left(\frac{nm}{ab}\right)\\ &= -\sum_{a|n,b|m,ab\neq 1}\mathbf{f}(a)\mathbf{f}(b)\times\mathbf{g}\left(\frac{n}{a}\right)\mathbf{g}\left(\frac{m}{b}\right)\end{aligned}$$

$$
\begin{aligned}
&= \mathbf{f}(1)\mathbf{f}(1) \times \mathbf{g}(n)\mathbf{g}(m) - \sum_{a|n}\sum_{b|m} \mathbf{f}(a)\mathbf{f}(b) \times \mathbf{g}\left(\frac{n}{a}\right)\mathbf{g}\left(\frac{m}{b}\right) \\
&= \mathbf{g}(n) \times \mathbf{g}(m) - \left(\sum_{a|n} \mathbf{f}(a)\mathbf{g}\left(\frac{n}{a}\right)\right) \times \left(\sum_{b|m} \mathbf{f}(b)\mathbf{g}\left(\frac{m}{b}\right)\right) \\
&= \mathbf{g}(n) \times \mathbf{g}(m) - \epsilon(n) \times \epsilon(m) \\
&= \mathbf{g}(n) \times \mathbf{g}(m) - [n = 1] \times [m = 1] \\
&= \mathbf{g}(n) \times \mathbf{g}(m)
\end{aligned}
$$

其中，在第三行，因为$ab \neq 1$，所以有$\frac{mn}{ab} < mn$，进而$\mathbf{g}\left(\frac{mn}{ab}\right)$可以直接运用归纳假设变换为$\mathbf{g}\left(\frac{n}{a}\right)\mathbf{g}\left(\frac{m}{b}\right)$．运用数学归纳法即得证． □

2.2 欧拉函数的性质

我们将**欧拉函数**$\varphi(n)$定义为小于n的正整数中与n互质的数的个数，即：

$$\varphi(n) = \sum_{i=1}^{n} [\gcd(n, i) = 1]$$

我们需要证明一下**欧拉函数是积性函数**.

证明：考虑有一个$x \perp nm$，就有$x \perp n$且$x \perp m$，就有$(p = x \bmod n) \perp n$且$(q = x \bmod m) \perp m$.

根据中国剩余定理，对于任意的一对$p \perp n$和$q \perp m$，都有唯一的$(x = ap + bq) \perp nm$，其中$a, b \in \mathbb{Z}^+$．于是就有当$n \perp m$时，$\varphi(n)\varphi(m) = \varphi(nm)$． □

还有一个结论：$\sum_{d|n} \varphi(d) = n$**对任意**$n \in \mathbb{Z}^+$**均成立，即**$\varphi * \mathbf{1} = \mathbf{id}$.

证明：首先，已经证明$\varphi * \mathbf{1}$是一个积性函数，所以我们只需考虑$\varphi(p^k)$的情况，其中p是一个质数．考虑写出当自变量在以上条件下的φ值：对于一个p^k，小于他的正整数中有且只有p的正整数倍和他不互质．所以就有：

$$\varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p - 1)$$

注意到上面的式子在$k = 0$时并不成立．将上面的式子套进我们要证的结论

中，得到：

$$\begin{aligned}
\sum_{d|p^k}\varphi(d) &= \sum_{i=0}^{k}\varphi(p^i) \\
&= \varphi(1)+\sum_{i=1}^{k}\varphi(p^i) && \text{(将}i=0\text{时的求和项提出来)} \\
&= 1+\sum_{i=1}^{k}p^{i-1}(p-1) && \text{(套用上述公式)} \\
&= 1+(p-1)\sum_{i=1}^{k}p^{i-1} \\
&= 1+(p-1)\cdot\frac{p^k-1}{p-1} && \text{(等比数列求和公式)} \\
&= 1+p^k-1=p^k
\end{aligned}$$

再套用前述的狄利克雷卷积性质即得证. □

3 莫比乌斯函数和莫比乌斯反演

3.1 莫比乌斯函数

我们将**莫比乌斯函数**μ定义为单位函数$\mathbf{1}$的逆元，即有$\mu * \mathbf{1} = \epsilon$. 按照这个定义，我们有

$$\sum_{d|n}\mu(d) = [n=1]$$

由于积性函数的逆元仍然是积性函数，我们只需要考虑$n=p^k$的情况，其中p是质数，k是非负数. 作为有逆元的积性函数，$\mu(1)$一定等于1；为了使$n=p^1$时上式仍成立，我们要使$\mu(p)$为-1；当$k\geq 2$时，μ的对应值就一定是0了.

把以上结论扩展，我们就得到了一个面对所有正整数的定义：我们设n分解后有k个质因数，他们是这样的

$$n = {p_1}^{s_1}\times {p_2}^{s_2}\times {p_3}^{s_3}\times\cdots\times {p_k}^{s_k} = \prod_{i=1}^{n}{p_i}^{s_i}$$

其中p_i为质数，$s_i \geq 1$，那么对应的莫比乌斯函数值就可以写成

$$\mu(n) = \begin{cases} 0 & (\text{存在一个} s_i > 1) \\ 1 & (k\text{为偶数}) \\ -1 & (k\text{为奇数}) \end{cases}$$

莫比乌斯函数除了具有其定义给出的性质之外，还具有一些神奇的性质，比如说，他和前述的欧拉函数φ就有着千丝万缕的联系．实际上，我们有下面的式子对于任意$n \in \mathbb{Z}^+$成立：

$$\varphi(n) = \sum_{d|n} \frac{n}{d} \cdot \mu(n) = \sum_{d|n} d \cdot \mu(\frac{n}{d})$$

将上式写成狄利克雷卷积的形式，我们得到：

$$\varphi = \mathbf{id} * \mu$$

证明：我们将已经证明的$\varphi * \mathbf{1} = \mathbf{id}$两边同时卷上一个$\mu$，得到：

$$\begin{aligned} \varphi * \mathbf{1} * \mu &= \mathbf{id} * \mu \\ \varphi * \epsilon &= \mathbf{id} * \mu \\ \varphi &= \mathbf{id} * \mu \end{aligned}$$

□

3.2 莫比乌斯反演

莫比乌斯反演公式：如果有两个函数$\mathbf{f}$和$\mathbf{g}$，他们满足$\mathbf{f}(n) = \sum_{d|n} g(d)$，那么就有：

$$\mathbf{g}(n) = \sum_{d|n} \mu(\frac{n}{d}) \cdot \mathbf{f}(d) = \sum_{d|n} \mu(d) \cdot \mathbf{f}(\frac{n}{d})$$

证明：我们把上式写成卷积的形式（即$f = \mathbf{1} * g$），然后在两边同时卷上一个μ：

$$\begin{aligned} \mathbf{f} * \mu &= \mu * 1 * g \\ \mathbf{f} * \mu &= \epsilon * 1 * g \\ \mathbf{f} * \mu &= g \end{aligned}$$

展开即得证．

□

4 杜教筛

4.1 推导

我们现在要求积性函数$\mathbf{f}$的前缀和，令我们要求的值为$\mathbf{S}(n)=\sum_{i=1}^{n}\mathbf{f}(i)$. 假设现在我们已经找到了另外两个积性函数$\mathbf{g}$和$\mathbf{h}$，使得$\mathbf{h}=\mathbf{f}*\mathbf{g}$. 现在，我们写出$\mathbf{h}$的前缀和的式子：

$$\begin{aligned}\sum_{i=1}^{n}\mathbf{h}(i)&=\sum_{i=1}^{n}(\mathbf{f}*\mathbf{g})(i)\\&=\sum_{i=1}^{n}\sum_{d|i}\mathbf{f}(\frac{i}{d})\cdot\mathbf{g}(d) && \text{(展开狄利克雷卷积)}\\&=\sum_{d=1}^{n}\mathbf{g}(d)\cdot\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\mathbf{f}(i) && \text{(交换求和号，用}i\text{枚举}\lfloor\frac{i}{d}\rfloor)\\&=\sum_{d=1}^{n}\mathbf{g}(d)\cdot\mathbf{S}(\lfloor\frac{n}{d}\rfloor)\\&=\mathbf{g}(1)\cdot\mathbf{S}(n)+\sum_{d=2}^{n}\mathbf{g}(d)\cdot\mathbf{S}(\lfloor\frac{n}{d}\rfloor) && \text{(把第一项提出来)}\end{aligned}$$

然后把$\mathbf{g}(1)\cdot\mathbf{S}(n)$扔到等号一边，得到：

$$\mathbf{g}(1)\cdot\mathbf{S}(n)=\sum_{i=1}^{n}\mathbf{h}(i)-\sum_{d=2}^{n}\mathbf{g}(d)\cdot\mathbf{S}(\lfloor\frac{n}{d}\rfloor)$$

其中$\mathbf{g}(1)$是1.

观察得到，以上的式子对我们选择$\mathbf{g}$和$\mathbf{f}$提出了要求：$\mathbf{h}$的前缀和要易于计算（一般是一个公式），同时$\mathbf{g}$的区间和也要可以用公式计算.

由于$\lfloor\frac{n}{i}\rfloor$在$i\in[1,n]$时只有$2\sqrt{n}$种取值（略证：$i$小于$\sqrt{n}$时只有$\sqrt{n}$个$i$，大于$\sqrt{n}$时只有$\sqrt{n}$个$\lfloor\frac{n}{i}\rfloor$），上面的式子计算一个积性函数的前缀和只需要一个低于$O(n)$的时间（实际上是$O(n^{\frac{3}{4}})$，和线性筛共同使用便可以达到$O(n^{\frac{2}{3}})$），具体的算法实现在此不再展开.

4.2 应用

我们接下来套用杜教筛算法写出计算φ，μ和$\mathbf{f}(n)=n\cdot\varphi(n)$的前缀和. 同样，我们只写出公式，不涉及具体的算法实现.

对于欧拉函数φ，我们很容易想到有$\varphi * \mathbf{1} = \mathbf{id}$；对于莫比乌斯函数$\mu$，我们也有$\mu * \mathbf{1} = \epsilon$．于是我们就可以得到：

$$\mathbf{S}_{\mu}(n) = 1 - \sum_{i=2}^{n} \mathbf{S}_{\mu}(\lfloor \frac{n}{i} \rfloor)$$

$$\mathbf{S}_{\varphi}(n) = \frac{n(n+1)}{2} - \sum_{i=2}^{n} \mathbf{S}_{\varphi}(\lfloor \frac{n}{i} \rfloor)$$

现在考虑第三个例子：$\mathbf{f}(n) = n \times \varphi(n)$，我们考虑把它和一个假想的$\mathbf{g}$卷上并展开：

$$\mathbf{h}(n) = (\mathbf{f} * \mathbf{g})(n) = \sum_{d|n} d \cdot \varphi(d) \cdot \mathbf{g}(\frac{n}{d})$$

我们考虑配一个$\mathbf{g} = \mathbf{id}$把多出来的这个d消掉：

$$\mathbf{h}(n) = \sum_{d|n} n \cdot \varphi(d) = n \cdot \sum_{d|n} \varphi(d) = n^2$$

我们就有答案了：

$$\mathbf{S}_{\mathbf{f}}(n) = \frac{n(n+1)(2n+1)}{6} - \sum_{i=2}^{n} i \cdot \mathbf{S}_{\mathbf{f}}(\lfloor \frac{n}{i} \rfloor)$$

对于后面的求和式中的i，我们套用等差数列求和公式即可．

参考文献

[1] 潘承洞、潘承彪，**初等数论**，北京大学出版社，第三版，2013年1月．

[2] Richard A. Brualdi；冯速等译，**组合数学**，机械工业出版社，第五版，2012年4月．

[3] Ronald L. Graham, Donald E. Knuth, Oren Patashnik；张明晓、张凡译，**具体数学**，人民邮电出版社，第二版，2013年4月．