Multiplicative functions and Möbius Inversion

Mostafa M. Mohamed

19 November, 2012

Disclaimer: The content of this document is a paraphrasing parts from the paper "Multiplicative Functions and Möbius Inversion Formula. Zvezdelina Stankova" in addition to parts from section 4.9 in "Concrete Mathematics. Donald Knuth". If there is a similarity in some sentences, it is mainly because some if the definitions and statements can be really short and concise.

Chapter 1

1.1 Multiplicative functions and Drichilet's product

Definition: $\mathcal{A}$ is the set of Arithmetic functions, and $\mathcal{M}$ is the set of Multiplicative functions, defined by:

$$\mathcal{A} = \{f : \mathbb{N} \to \mathbb{C}\}$$

$$\mathcal{M} = \{f \in \mathcal{A} | f(1) = 1 \wedge (m \perp n \Rightarrow f(mn) = f(m)f(n))\}$$

The arithmetic functions:

- $\tau(n)$ = number of divisors of n
- $\sigma(n)$ = sum of divisors of n
- $\sigma_k(n)$ = sum of k^{th} powers of divisors of n
- $\rho(n)$ = product of divisors of n

Can be defined by:

$$\tau(n) = \sum_{d|n} 1, \quad \rho(n) = \prod_{d|n} d$$

$$\sigma(n) = \sum_{d|n} d, \quad \sigma_k(n) = \sum_{d|n} d^k$$

The functions τ, σ, σ_k are multiplicative functions, while ρ is not multiplicative. If we have a number n with prime factorization $n = p_1^{e_1} \cdots p_r^{e_r}$, and a multiplicative function f, then we have $f(n) = f(p_1^{e_1}) \cdots f(p_r^{e_r})$, and if we have a set of multiplicative functions $f_1, \cdots, f_r$, then the product $f_1 \cdots f_r$ is a multiplicative function.

Definition: Sum function of an arithmetic function $f(n)$ is defined as

$$S_f := \sum_{d|n} f(d)$$

Theorem: $S_f(n)$ is multiplicative if and only if $f(n)$ is multiplicative.

(1.1)

Theorem: If $f(n)$ is a multiplicative function and the prime factorization of $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$S_f(n) = \prod_{i=1}^{r} \sum_{k=0}^{e_i} f(p_i^k) \tag{1.2}$$

1.2 Drichilet's product

Definition: Drichilet's Product is a binary operation defined on the set of arithmetic functions as follows

$$f \circ g(n) := \sum_{d|n} f(d) g(\frac{d}{n})$$

or equivalently,

$$f \circ g(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

- Drichilet's product is Commutative.

$$f \circ g(n) = g \circ f(n) \tag{1.3}$$

- Drichilet's product is Associative.

$$f \circ (g \circ h)(n) = (f \circ g) \circ h(n) = f \circ g \circ h(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3) \tag{1.4}$$

- Drichilet's product is closed under arithmetic functions. The proof follows from the definition.

(1.5)

- Drichilet's product is closed under multiplicative functions.
  Proof : Given two multiplicative functions f, g and two coprime numbers n, m.

$$f \circ g(nm) = \sum_{d|nm} f(d) g(\frac{nm}{d}) = \sum_{d_1|n, d_2|m, d_1 d_2 = d} f(d_1 d_2) g(\frac{n}{d_1} \frac{m}{d_2})$$

$$= \sum_{d_1|n, d_2|m} f(d_1) f(d_2) g(\frac{n}{d_1}) g(\frac{m}{d_2})$$

$$= \sum_{d_1|n} f(d_1) g(\frac{n}{d_1}) \sum_{d_2|m} f(d_2) g(\frac{m}{d_2}) = f \circ g(n) \cdot f \circ g(m) \tag{1.6}$$

1.3 Multiplicative functions groups

We define three functions, that are multiplicative:

- $I(n) = 1$
- $id(n) = n$

- $e(n) = \delta_1^n$

(1.7)

We can find that:

$$f \circ I(n) = S_f(n),\ f \circ e(n) = f(n) \tag{1.8}$$

Since we have an identity function for Drichilet's product, we can define an inverse on Drichilet's product.
Definition: If there is a function g such that

$$f \circ g(n) = g \circ f(n) = e(n),$$

then g is an inverse of f, denoted by $g = f^{-1}$
Theorem: If a given Arithmetic function is invertible, then it's inverse is unique.
Proof: Suppose we have g, h such that $f \circ g = f \circ h = e$, then we have

$$h = h \circ e = h \circ f \circ g = e \circ g = g \tag{1.9}$$

An Arithmetic function f is invertible if and only if $f(1) \neq 0$, and it's inverse is given recursively for $1 < n$ by:

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d<n, d|n} f(\frac{n}{d}) f^{-1}(d),\ f^{-1}(1) = \frac{1}{f(1)} \tag{1.10}$$

Theorem: Given an invertible arithmetic function $f(n)$, $f(n)$ is multiplicative if and only if $f^{-1}(n)$.

(1.11)

The group $(\mathcal{A}^\circ, \circ)$ forms an abelian group, and the group $(\mathcal{M}, \circ)$ forms an abelian subgroup of it. The proof follows from 1.3, 1.4, 1.6, 1.7, 1.9, 1.11.

1.4 Möbius and Euler functions

We introduce two crucial Multiplicative functions μ and ϕ.

- Möbius function $\mu(n)$ is a multiplicative function (proof follows from 1.11), which is defined by:
$$\mu(n) := I^{-1}(n)$$
- Euler's Totient Function $\phi(n)$, which is defined by:
$$\phi(n) := |\{m \leq n | m \perp n\}|$$

  Proof: Using the number theoretic property, for all m, n that are coprimes and integer x:

  $$(x \bmod mn) \perp mn \textit{ if and only if } (x \bmod m) \perp m \text{ and } (x \bmod n \perp n)$$

  This statement shows that for every $x \leq mn$, there's a unique pair (a, b) where $a \leq n \wedge b \leq m$, such that the $coprimes(mn)$ is bijective

to $coprimes(n) \times coprimes(m)$, The bijection can be deduced by using Chinese remainder theorem:

$$f(a,b) = (am + bn) \bmod mn, f^{-1}(x) = (x \bmod n, x \bmod m)$$

Thus we can conclude that both sets have equal sizes, implying that Euler's Totient function is multiplicative.

1.5 Computing Möbius and Euler functions

1.5.1 Computing μ

Möbius function can be computed by:

$$\mu(n) = \begin{cases} (-1)^r & n = p_1 \cdots p_r \\ 0 & n \text{ is not square-free} \end{cases}$$

Proof: By the definition of μ, if we have a prime p, we get that $\sum_{d|p^k} \mu(p^k) = e(p^k)$, which is equivalent to $\sum_{i=0}^{k} \mu(p^i) = \delta_0^k$, which implies that $\mu(1) = 1, \mu(p) = -1$ and $k > 1 \Rightarrow \mu(p^k) = 0$, Since $\mu(n)$ is multiplicative, we can use this fact to compute $\mu(n)$, thus $\mu(n) = 0$ if n is not square-free, otherwise $\mu(n) = (-1)^r$ where r is the number of prime divisors for n.

1.5.2 Computing ϕ

If we have $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$$

Proof: By the definition of ϕ, if we have a prime p, all the numbers excluding the multiples of p are coprimes with p^k, that we get that $\phi(p^k) = p^k - p^{k-1}$. Using 1.1, 1.2 we can deduce the rest of the proof.

Theorem: $\phi \circ I(n) = n$
Proof: By using the formula obtained for $\phi(n)$, if we have a prime p, then $\sum_{d|p^k} \phi(d) = \sum_{i=0}^{k} \phi(p^i) = 1 + (p-1)\sum_{i=0}^{k} p^i = p^k$, and since ϕ is multiplicative, we use statement 1.1, 1.2 to deduce the stated assertion.

1.6 Möbius Inversions

Möbius Inversion Formula If we have two multiplicative functions g, f such that $g = f \circ I$, then we have:

$$g(n) = f \circ I(n) \iff f(n) = g \circ \mu(n) \tag{1.12}$$

equivalently,

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(d) f(n/d) \tag{1.13}$$

Another useful form of the inversion formula (which is a special case of the generalized formula 1.6.1):

$$f(n) = \sum_{k=1}^{n} g(\lfloor \frac{n}{k} \rfloor) \Longleftrightarrow g(n) = \sum_{k=1}^{n} \mu(k) f(\lfloor \frac{n}{k} \rfloor) \tag{1.14}$$

1.6.1 Generalized Möbius Inversion Formula

Suppose that $\sum_{k,d\geq 1} |g(x_1/kd, \cdots, x_r/kd)|$ and $\sum_{k,d\geq 1} |f(x_1/kd, \cdots, x_r/kd)|$ converges

$$f(x_1, \cdots, x_r) = \sum_{k=1}^{\infty} g(\frac{x_1}{k}, \cdots, \frac{x_r}{k}) \Longleftrightarrow g(x_1, \cdots, x_r) = \sum_{k=1}^{\infty} \mu(k) f(\frac{x_1}{k}, \cdots, \frac{x_r}{k}) \tag{1.15}$$

Proof $\Rightarrow$:

$$\sum_{k=1}^{\infty} \mu(k) f(\frac{x_1}{k}, \cdots, \frac{x_r}{k}) = \sum_{k=1}^{\infty}\sum_{i=1}^{\infty} \mu(k) g(\frac{x_1}{ki}, \cdots, \frac{x_r}{ki}) = \sum_{m=1}^{\infty} g(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) \sum_{k=1}^{\infty}\sum_{i=1}^{\infty} \mu(k)[m = ki]$$

$$= \sum_{m=1}^{\infty} g(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) \sum_{k|m} \mu(k) = \sum_{m=1}^{\infty} g(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) e(m) = g(x_1, \cdots, x_r)$$

Proof $\Leftarrow$:

$$\sum_{k=1}^{\infty} g(\frac{x_1}{k}, \cdots, \frac{x_r}{k}) = \sum_{k=1}^{\infty}\sum_{i=1}^{\infty} \mu(i) f(\frac{x_1}{ki}, \cdots, \frac{x_r}{ki}) = \sum_{m=1}^{\infty} f(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) \sum_{k=1}^{\infty}\sum_{i=1}^{\infty} \mu(i)[m = ki]$$

$$= \sum_{m=1}^{\infty} f(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) \sum_{i|m} \mu(i) = \sum_{m=1}^{\infty} f(\frac{x_1}{m}, \cdots, \frac{x_r}{m}) e(m) = f(x_1, \cdots, x_r)$$

1.6.2 Counting coprime tuples

Definition: $f_r(n, k)$ is the number r-tuples of integers $\leq n$ that has a greatest common divisor k. That is:

$$f_r(n, k) = |\{(m_1, \cdots, m_r) | \gcd(m_1, \cdots, m_r) = k \wedge m_i \leq n\}|$$

This function can also be computed by:

$$f_r(n, k) = f_r(\lfloor \frac{n}{k} \rfloor, 1)$$

This form helps us to deduce an efficient way to compute the number of coprime r-tuples using:

$$\sum_{k=1}^{n} f_r(n, k) = n^r = \sum_{k=1}^{n} f_r(\lfloor \frac{n}{k} \rfloor, 1)$$

then by applying the generalized Möbius inversion formula on it we get:

$$f_r(n, 1) = \sum_{k=1}^{n} \mu(k) (\lfloor \frac{n}{k} \rfloor)^r$$