The Möbius Function and Möbius Inversion

Sydney Wong

May 4, 2015

1 Introduction

The Möbius function $\mu(n)$ is an important multiplicative function used in many fields, but mainly in number theory and combinatorics. It was first defined, in an implicit form, by Leonhard Euler [3]. More than 100 years later, in 1831, German mathematician August Ferdinand Möbius explicitly defined it and studied its properties in his paper *Über eine besondere Art von Umkehrung der Reihen* [4]. The Möbius inversion formula was developed much later, in the 1930s, but Möbius's name is still attached to it [9]. The aim of this paper is to present the Möbius function and Möbius inversion and a generalization of it, along with some historical information and applications.

2 Dirichlet Convolution

Some of our preliminary proofs and results use Dirichlet convolution, so we will present it and some of its properties here.

An arithmetic function is a real or complex valued function defined on the set of natural numbers. If f and g are two arithmetic functions, one can define a new arithmetic function $f * g$, the Dirichlet convolution of f and g, by

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

Dirichlet convolution was developed by Peter Gustav Lejeune Dirichlet, who lived from 1805 to 1859 and worked in Göttingen between 1855 and 1859 [6]. Dirichlet was in Göttingen long after Möbius had already left, but since they both worked with Johann Carl Friedrich Gauss, they may have influenced each other's work indirectly. One can think of Dirichlet convolution as giving a binary operation on the set of arithmetical functions, an idea that was first introduced by E.T. Bell [1] and M. Cipolla [2].

Lemma 2.1. *Dirichlet convolution is commutative and associative.*

Proof. It is convenient to rewrite Dirichlet convolution in a symmetric form:

$$(f * g)(n) = \sum_{ab=n} f(a)\, g(b)$$

The sum extends over all pairs of positive integers a, b, whose product is n. So clearly Dirichlet convolution is commutative. As for associativity, we have

$$\begin{aligned}((f*g)*h)(n) &= \sum_{ab=n} (f*g)(a)\,h(b) \\ &= \sum_{ab=n} \left[\sum_{cd=a} f(c)\,g(d)\right] h(b) \\ &= \sum_{bcd=n} f(c)g(d)h(b)\end{aligned}$$

and

$$\begin{aligned}(f*(g*h))(n) &= \sum_{ab=n} f(a)\,(g*h)(b) \\ &= \sum_{ab=n} f(a) \left[\sum_{cd=b} g(c)h(d)\right] \\ &= \sum_{acd=n} f(a)g(c)h(d)\end{aligned}$$

By commutativity of Dirichlet convolution, $\sum_{bcd=n} f(c)g(d)h(b) = \sum_{acd=n} f(a)g(c)h(d)$ so Dirichlet convolution is also associative. □

Define an arithmetic function e such that

$$e(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Lemma 2.2. *e is the Dirichlet identity, meaning $f*e = e*f = f$ for all arithmetic functions f.*

Proof.

$$(f*e)(n) = \sum_{d|n} f(d)\,e\left(\frac{n}{d}\right)$$

$e\left(\frac{n}{d}\right)$ equals 1 if and only if $n = d$, so the right hand side of the above equality reduces to $f(n)$. □

3 The Möbius Function

Definition 3.1. *The Möbius function is defined as* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ *where*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ different prime numbers} \\ 0 & \text{if } n \text{ is divisible by the square of a prime number} \end{cases}$$

The Möbius function is *multiplicative*, meaning

$$\mu(ab) = \mu(a)\,\mu(b) \text{ if } gcd(a, b) = 1$$

Theorem 3.2. $\mu(n)$ *has the property that*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof. If $n = 1$, $\sum_{d|n} \mu(d) = \mu(1) = 1$. Now suppose n has k distinct prime factors, meaning $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where p_i are prime and $\alpha_i \in \mathbb{N}$. Each divisor of n (other than 1) is a product of some unique combination of the p_i. So for n,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i < j \le k}^{k} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \dots p_k) \\ &= 1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= \sum_{i=0}^{k} \binom{k}{i}(-1)^i \\ &= (1-1)^k = 0 \end{aligned}$$

□

Define an arithmetic function 1 such that $1(n) = 1\ \forall n$.

Lemma 3.3. *The Dirichlet inverse of the function* $1(n)$ *is the Möbius function* $\mu(n)$*, meaning* $\mu * 1 = 1 * \mu = e$.

Proof.

$$\begin{aligned} (\mu * 1)(n) &= \sum_{d|n} \mu(d)\, 1\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d) \\ &= e(n) \end{aligned}$$

□

Let f be an arithmetic function. Then f is totally multiplicative if $f(nm) = f(n) f(m)$ for all n and m.

Lemma 3.4. *If f is totally multiplicative and $f(1) \neq 0$ then its Dirichlet convolution inverse is $f^{-1} = \mu f$.*

Proof.

$$(\mu f * f)(n) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right)$$

Because f is totally multiplicative, $f(d) f\left(\frac{n}{d}\right) = f(n)$. So then we have

$$\begin{aligned}(\mu f * f)(n) &= \sum_{d|n} \mu(d) f(n) \\ &= f(n) \sum_{d|n} \mu(d)\end{aligned}$$

By Theorem 3.2, $\sum_{d|n} \mu(d)$ equals 1 for $n = 1$ and equals 0 for $n > 1$. If $f(1) = 0$, then the right hand side is the zero function. So as long as $f(1) \neq 0$, which was one of our original conditions, the right hand side equals $e(n)$. So μf is the inverse of f. □

4 Möbius Inversion

The formula for Möbius inversion was first obtained by Louis Weisner in 1935 and was also noticed by Philip Hall independently in 1936 [9]. So Möbius inversion was actually developed long after Möbius's time.

Theorem 4.1. *(Möbius Inversion) If f and g are arithmetic functions satisfying*

$$g(n) = \sum_{d|n} f(d) \text{ for every integer } n \geq 1$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) \text{ for every integer } n \geq 1$$

where μ is the Möbius function and d is a positive divisor of n.

Proof. Van Lint and Wilson present the following proof [10].

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} f(d') \\ &= \sum_{d'|n} f(d') \sum_{m|(n/d')} \mu(m)\end{aligned}$$

By Theorem 3.2, $\sum_{m|(n/d')} \mu(m)$ is 0 unless $d' = n$, in which case this sum equals 1. Thus the right hand side reduces to $\sum_{d'|n} f(d') = f(n)$. So $\sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = f(n)$, and the proof is complete. $\square$

Theorem 4.2. *In terms of Dirichlet convolution, the Möbius inversion formula can be written as*

$$\text{if } g = f * 1 \text{ then } f = \mu * g,$$

where 1 *is the constant function* $1(n) = 1$.

Proof. Using the fact that Dirichlet convolution is associative, we can say

$$\mu * g = \mu * (1 * f) = (\mu * 1) * f = e * f = f$$

$\square$

5 Generalizations of Möbius Inversion

The Möbius function and Möbius inversion presented in the previous two sections is actually a number-theoretic application of a related inversion formula that is more useful in combinatorics. A more general form of the Möbius function and Möbius inversion, as developed by Gian Carlo Rota in 1964, is applied to locally finite partially ordered sets [9]. The same was done by Harold Scheid independently in 1968 [9]. Van Lint and Wilson [10] present the Möbius function and Möbius inversion as applied to posets in the following way:

Let P be a locally finite partially ordered set. Because P is locally finite, it means that for all $x, y \in P$, the interval $[x, y]$ consists of finitely many elements. The incidence algebra $\mathbb{A}(P)$ consists of all matrices α such that $\alpha(x, y) = 0$ unless $x \leq y$ in P. By the definition of matrix multiplication,

$$(\alpha\beta)(x, y) = \sum_{z \in P} \alpha(x, z)\beta(z, y).$$

For $\alpha, \beta \in \mathbb{A}(P)$, the above sum needs to be extended over only those z in the interval $[x, y]$ meaning $x \leq z \leq y$, because for other values of z, either $\alpha(x, z)$ or $\beta(z, y)$, or both, will be 0. Define a function ζ to be

$$\zeta(x, y) = \begin{cases} 1 & \text{if } x \leq y \text{ in } P \\ 0 & \text{otherwise} \end{cases}$$

ζ is invertible and its inverse, the Möbius function of P, will be denoted by μ. The condition $\zeta\mu = I$ requires that

$$\sum_{x \leq z \leq y} \mu(x, z) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

This is true if we define μ inductively, by declaring $\mu(x, x) = 1$, $\mu(x, y) = 0$ if $x \not\leq y$, and $\mu(x, y) = -\sum_{x \leq z \leq y} \mu(x, z)$ for $x < y$ in P.

Note that the number-theoretic versions of the Möbius function and Möbius inversion presented in the previous two sections take the poset $(\mathbb{N}, \text{divides})$.

6 Applications of Möbius Inversion

6.1 Euler Totient Function

Euler's totient function, which was first introduced in 1763 and is denoted as $\phi(n)$, counts the positive integers less than or equal to n that are relatively prime to n. It states that

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

Lemma 6.1. $\phi(n) = \sum\limits_{d|n} d \cdot \mu\left(\frac{n}{d}\right)$

Proof. We can multiply out the product to get

$$\begin{aligned}
\phi(n) &= n\left[1 - \frac{1}{p_1} - \frac{1}{p_2} \cdots + \frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} \ldots\right] \\
&= n\left[\sum_{d|n} \frac{\mu(d)}{d}\right] \\
&= \sum_{d|n} \mu(d)\left(\frac{n}{d}\right) \\
&= \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right)
\end{aligned}$$

□

Proposition 6.2. $\sum\limits_{d|n} \phi(d) = n$, *where the sum is over all positive divisors d of n.*

Proof. We will prove this using Möbius inversion. Define a function g, such that

$$g(n) = n \text{ for every integer } n.$$

Then, using Lemma 6.1,

$$\begin{aligned}
\phi(n) &= \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right) \\
&= \sum_{d|n} g(d) \cdot \mu\left(\frac{n}{d}\right)
\end{aligned}$$

Therefore, using Möbius inversion,

$$g(n) = \sum_{d|n} \phi(d)$$

□

Proposition 6.3. $\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$

Proof. From Lemma 6.1, we have $\phi(n) = \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right)$. Using the commutativity of Dirichlet convolution, we have $\phi(n) = \sum_{d|n} \frac{n}{d} \cdot \mu(d)$. Divide both sides by n and the proof is complete. □

Proposition 6.2 is a property established by Gauss in his *Disquisitiones Arithmeticae* of 1801 [7]. In 1813, Möbius travelled to Göttingen where he was a student of astronomy under Gauss [4]. It would not be surprising if Gauss influenced and inspired some of Möbius's work.

6.2 Pólya Enumeration Theorem

The Pólya Enumeration Theorem, which is not explicitly presented here, was published by George Pólya in 1937 [8]. We will present an example that is similar to one that Van Lint and Wilson [10] presented. Define $N(n)$ to be the number of necklaces of white and black beads of length n, where two necklaces obtained by a rotation are considered the same. Let $M(d)$ be the number of necklaces with period d, where period is defined as the number of times the necklace can be rotated before it gets back to its original configuration.

Lemma 6.4. $nM(n) = \sum_{d|n} \mu(d)\, 2^{n/d}$

Proof. First note that $N(n) = \sum_{d|n} M(d)$. If we consider two necklaces obtained by a rotation to be different, we get the result $\sum_{d|n} d \cdot M(d) = 2^n$ since this counts all possible necklaces. Now we will apply Möbius inversion (Theorem 4.1). Define $g(n) = 2^n$ and $f(n) = n \cdot M(n)$. Then, since $2^n = \sum_{d|n} d \cdot M(d)$, we have $g(n) = \sum_{d|n} f(d)$. So Theorem 4.1 gives $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$ which means $nM(n) = \sum_{d|n} \mu(d) 2^{n/d}$. □

Proposition 6.5. $N(n) = \frac{1}{n} \sum_{l|n} \phi\left(\frac{n}{l}\right) 2^l$

Proof.

$$\begin{aligned} N(n) &= \sum_{d|n} M(d) \\ &= \sum_{d|n} \frac{1}{d} \sum_{l|d} \mu(l)\, 2^{(d/l)} \\ &= \sum_{d|n} \frac{1}{d} \sum_{l|d} \mu\left(\frac{d}{l}\right) 2^l \end{aligned}$$

Now write $k = \frac{d}{l}$ (so that $d = kl$) and reorder so that the sum over $l|n$ is on the outside.

$$\begin{aligned} N(n) &= \sum_{d|n} \frac{1}{d} \sum_{l|d} \mu\left(\frac{d}{l}\right) 2^l \\ &= \sum_{l|n} \sum_{k|(n/l)} \frac{1}{kl}\, \mu(k)\, 2^l \\ &= \sum_{l|n} \frac{2^l}{l} \sum_{k|(n/l)} \frac{\mu(k)}{k} \end{aligned}$$

Using Proposition 6.3 we know that $\sum\limits_{k|(n/l)} \frac{\mu(k)}{k} = \frac{\phi\left(\frac{n}{l}\right)}{\frac{n}{l}}$, so we have

$$\begin{aligned} N(n) &= \sum_{l|n} \frac{2^l}{l} \sum_{k|(n/l)} \frac{\mu(k)}{k} \\ &= \sum_{l|n} \frac{2^l}{l} \frac{\phi\left(\frac{n}{l}\right)}{\frac{n}{l}} \\ &= \frac{1}{n} \sum_{l|n} \phi\left(\frac{n}{l}\right) 2^l \end{aligned}$$

$\square$

Proposition 6.5 can also be proven using Burnside's Lemma, of which the Pólya Enumeration Theorem is a generalization.

6.3 Riemann Zeta Function

Georg Friedrich Bernhard Riemann lived from 1826 to 1866. In 1846 he began his attendance at the University of Göttingen, where he studied under Gauss. He only stayed in Göttingen for a short time, for in 1847 he moved to Berlin University where he worked with many people, including Dirichlet [5]. The Riemann ζ-function is defined as $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$.

Proposition 6.6.

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

Proof. Letting p_i denote the ith prime, the Euler product expression for ζ is

$$\begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots \end{aligned}$$

Euler used a sieving method on this infinite sum to remove elements that have the factors $\frac{1}{p_i^s}$. For example, if we divide each term in the infinite sum by 2^s we get

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \ldots$$

Then if we subtract this equation from $\zeta(s)$ we get

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \ldots$$

Repeating this process infinitely, the sum will be sieved until it equals 1, at which time the left hand side will contain a product over all the prime numbers. Thus,

$$\zeta(s) = \prod_{i=1}^{\infty}\left(\frac{1}{1 - \frac{1}{p_i^s}}\right)$$

So then we see that

$$\frac{1}{\zeta(s)} = \prod_{i=1}^{\infty}\left(1 - \frac{1}{p_i^s}\right)$$

A Dirichlet series is any series of the form $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$. A series $F(s)$ is said to be generated by a function f if $F(s) = \frac{f(n)}{n^s}$. Suppose f generates the Dirichlet series $\zeta(s)$. Then, by Lemma 3.4, $\zeta(s)^{-1}$ is the Dirichlet series generated by μf. So

$$\frac{1}{\zeta(s)} = \prod_{i=1}^{\infty}\left(1 - \frac{f(p_i)}{p_i^s}\right)$$

where $f(n) = 1(n)$. So $\zeta(s)^{-1}$ is the Dirichlet series generated by $\mu \cdot 1$, and by the definition of Dirichlet series, we have

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$$

□

7 Conclusion

The Möbius function and Möbius inversion have become important tools in many areas including combinatorics and number theory since they were introduced into the mathematical community. Applying Möbius inversion to posets that we have not covered in this paper (including the lattice of all subsets of an n-set, the lattice of all subspaces of a finite-dimensional vector space over a finite field, the lattice of all partitions of an n-set, the lattice of faces of a convex polytope, etc.) results in important concepts such as inclusion-exclusion [10].

Möbius was a colleague of Hermann Günter Grassmann and in 1844 they worked together [4]. Because of Grassmann's interest in linear subspaces of finite-dimensional vector spaces over a finite field, and the fact that Möbius inversion is now applied to those, it would not be surprising if this overlap was not pure coincidence. Möbius inversion is arguably one of the most utilized and powerful theorems in combinatorics. It permeates many different fields of mathematics and society will definitely see more developments inspired by it. The discovery of the number-theoretic theorem, followed by its subsequent generalization to functions of posets, is a prime example of how mathematics frequently progresses. Old discoveries are often found to be special cases of broader truths, and later applications of a theorem may be far removed from the field in which it was originally derived.

References

[1] E.T. Bell, An arithmetical theory of certain numerical functions, *Univ. Wash. Publ. Math. Phys. Sci.*, **I**:1,(1915), encyclopediaofmath.org

[2] M. Cipolla, Sui principi del calculo arithmetico integrale *Atti Accad. Gioenia Cantonia*, **5**:8,(1915), encyclopediaofmath.org

[3] N.C. Negoescu, *Generalizations of the Möbius' Theorem of Inversion*, Editura Waldpress, 1995

[4] J.J. O'Connor and E.F. Robertson, *August Ferdinand Möbius*, School of Mathematics and Statistics, University of St. Andrews, Scotland, 1997

[5] J.J. O'Connor and E.F. Robertson, *Georg Friedrich Bernhard Riemann*, School of Mathematics and Statistics, University of St. Andrews, Scotland, 1998

[6] J.J. O'Connor and E.F. Robertson, *Johann Peter Gustav Lejeune Dirichlet*, School of Mathematics and Statistics, University of St. Andrews, Scotland, 2000

[7] M. Plytage, P. Loomis, and J. Polhill, Summing Up the Euler ϕ Function, *The College Mathematics Journal*, **39**, 34-42, (2008)

[8] G. Pólya, Kombinatorische Anzahlbestimmungen fr Gruppen, Graphen und chemische Verbindungen, *Acta Math*, **68**, 145-254, (1937), encyclopediaofmath.org

[9] R. Sivaramakrishnan, *Certain Number-Theoretic Episodes in Algebra*, CRC Press, 2007

[10] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992, 2001