From Posets to Derangements:

An Exploration of the Möbius Inversion Formula

Allison Beemer

May 14, 2012

Acknowledgements

I would like to thank Professors David Guichard and Barry Balof for their support and guidance through this process. Also, a huge thank you to all of my classmates, but especially to Mollee Huisinga for her wonderful feedback and endless supply of encouraging stickers.

Introduction

We are surrounded by partially ordered sets, though we rarely view them as such. We will formally define partially ordered sets, or posets, in the first section of this paper, but for now, consider the following example: a family tree is a set of objects (the family members) together with a relation (pun intended) defined on the elements of the set. For example, you could say that a person a is "$\leq$" a person b if they are a direct descendant of b. Say person a is person b's sister. Neither is a descendant of the other, so they are not related (according to "$\leq$"). This is a non-numeric partially ordered set. Given the obvious relevance of such sets, it is only natural that we should wish to investigate functions defined on them.

In this paper, we begin with a simple seed of an idea, that of a partially ordered set. We proceed by considering properties of compatible matrices, walking through a proof of the existence and uniqueness of what is known as the Möbius function, μ, and subsequently offering a proof of the Möbius inversion formula. The development of the Möbius function and the proof of the Möbius inversion formula lead to results in several branches in mathematics, including combinatorics and number theory. In combinatorics, the Möbius inversion formula implies the principle of inclusion and exclusion, which is a tool used to count the number of elements of a given set in a somewhat inverted way. The Möbius function and inversion formula may also be defined number theoretically and used to prove a plethora of results. For example, we will discuss an explicit formula for counting the number of integers less than a given integer that are relatively prime to that integer. In addition to a certain level of mathematical know-how, we will assume, on the part of our reader, a working knowledge of basic set theory – including familiarity with set unions and intersections – as well as a firm understanding of basic operations on matrices.

1 Partially Ordered Sets

When asked to imagine an ordered set, most moderately informed students of mathematics would picture a set with a total ordering relation. That is, if we chose any two elements in their set, they would be related by the ordering relation on the set. For instance, consider the integers with the

ordering relation $\leq$. Given any two integers a and b, either $a \leq b$ or $b \leq a$. Suppose, instead, that we have an ordered set where it is not guaranteed that two given elements will be related at all. Such sets, called partially ordered sets, or posets, will be essential to our discussion, and are defined formally below.

1.1 Definitions and Examples

Definition 1.1. [3, p.353] A relation $\leq$ on a set S is called a *partial order*, or a *partial ordering relation*, if $\leq$ is reflexive, antisymmetric, and transitive.

As a quick review, recall that a relation $\leq$ on S is said to be *reflexive* if $x \leq x$ for all $x \in S$, *antisymmetric* if exactly one of $x \leq y$ or $y \leq x$ is true for distinct $x, y \in S$, and *transitive* if $x \leq y \wedge y \leq z$ implies that $x \leq z$ for $x, y, z \in S$.

Definition 1.2. [3, p.372] The pair $(S, \leq)$ is called a *partially ordered set*, or *poset*, if the relation $\leq$ on the set S is a partial ordering relation.

Partially ordered sets can take numerous forms. For example, we could have a partially ordered set comprised of the set $S = \{2, 3, 6, 7\}$, and the partial ordering relation "divides," so that $d_1 \leq d_2$ if $d_1 | d_2$ for d_1, $d_2 \in S$. Clearly, $2|6$, but 3 and 7 are not related.

In order to visualize partially ordered sets, we may use what are called Hasse diagrams, which are defined as follows:

Definition 1.3. [3, p.373] If $\leq$ is a partial order on a finite set V, we construct a *Hasse diagram* for $\leq$ on V by drawing a line segment from x up to y if x, $y \in V$ with $x \leq y$ and if there is no other element $z \in V$ such that $x \leq z$ and $z \leq y$. (So there is nothing "in between" x and y.)

For example, Figure 1 helps us to see the partial ordering relation $\subseteq$ on $\mathcal{P}(\{a, b, c\})$. Note that $\mathcal{P}(\{a, b, c\})$ denotes the power set of $\{a, b, c\}$, which is the set of all subsets of the set $\{a, b, c\}$. We may travel (strictly "vertically") between $\{a\}$ and $\{a, b, c\}$, and so, sure enough, $\{a\} \subseteq \{a, b, c\}$. However, we may not travel in this fashion between $\{a, b\}$ and $\{c\}$. So, $\{a, b\}$ and $\{c\}$ are not related.

1.2 A Nice Property of Partially Ordered Sets

Let $V = \{x_1, x_2, \ldots, x_n\}$, together with the partial ordering relation $\leq$, be a partially ordered set.

We propose that we may take the elements of V and create an ordered list so that if, for integers i and j between 1 and n, x_i falls to the left of x_j in our list, then $x_j \not\leq x_i$.

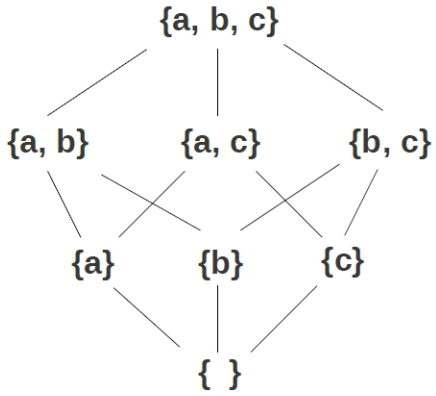

Figure 1: The Hasse diagram for the partially ordered set $(V, \subseteq)$, where $V = \mathcal{P}(\{a, b, c\})$.

To show that we may do this, we use the principle of mathematical induction on the number of elements in our partially ordered set.

Proof. As our base case, consider a partially ordered set defined by a set containing two elements and the partial ordering relation $\leq$. Then, these two elements, call them a and b, either have no relation, or exactly one of $a \leq b$, $b \leq a$ is true. Notice that we may write our two elements in list form as $[a, b]$ (or $[b, a]$) if they have no relation, $[a, b]$ if $a \leq b$, or $[b, a]$ if $b \leq a$. It is easy to see that these listings satisfy the necessary condition.

Next, suppose that we may list the elements as desired for a partially ordered set defined by a set containing k elements and the partial ordering relation $\leq$. Call the set of k elements V_k. Then, we will add one more element to the set. We claim that we can place this element so that the resulting list of $k + 1$ elements has the desired properties.

Consider the sets:

$$S = \{x_i : x_i \in V_k, x_i \leq x_{k+1}\}$$
$$T = \{x_i : x_i \in V_k, x_{k+1} \leq x_i\} \ .$$

Notice that the union of these two sets is comprised of all elements in V_k which are related to $k+1$, and that this union is a (not necessarily proper) subset of V_k.

If either S or T is the empty set, place x_{k+1} at the far left or right end of the list, respectively. It is clear that this new list of $k + 1$ elements satisfies our conditions, and we are done.

Otherwise, there are finitely many elements in each set, so there exists an element of S that is farthest to the right in our ordered list of V_k, and, similarly, there exists an element of T that is farthest to the left in our list.

Call these elements x_s and x_t, respectively. We claim that x_s is to the left of x_t on our list of V_k, and that we may place x_{k+1} anywhere between x_s and x_t to obtain a list of V_{k+1} with the desired properties.

Because $x_s \leq x_{k+1}$ and $x_{k+1} \leq x_t$ by our definitions of S and T, and the partial ordering relation $\leq$ is transitive by definition, we find that $x_s \leq x_t$. Since it cannot be the case that x_s is to the right of x_t, it follows that x_s must be to the left of x_t. We can thus place x_{k+1} between x_s and x_t. We claim that this is an ordered list of V_{k+1}.

(Aside: Because this is a rather abstract argument, we will give a brief example of how this inductive step might work. Let $V_k = \{\emptyset, \{a\}, \{a, c\}, \{b\}, \{a, b, c\}\}$, and let $\subseteq$ be the partial ordering relation on V_k. Then, we may order V_k in the desired way as: $\emptyset, \{a\}, \{b\}, \{a, c\}, \{a, b, c\}$ or $\emptyset, \{b\}, \{a\}, \{a, c\}, \{a, b, c\}$. If we want to introduce the element $\{c\}$, we note that the set S, as defined above, is equal to $\{\emptyset\}$, and the set T, also as defined above, is equal to $\{\{a, c\}, \{a, b, c\}\}$. So, we may place $\{c\}$ anywhere between $\emptyset$ and $\{a, c\}$ in either of our above ordered lists and have a new ordered list that includes $\{c\}$ and satifies our desired properties. For example, $\emptyset, \{b\}, \{c\}, \{a\}, \{a, c\}, \{a, b, c\}$ is one such final ordering.)

We will now show that we have created an ordered list of V_{k+1} with the desired properties. Suppose that $x_{k+1} \leq x_m$ for some integer m between 1 and k.

Then, $x_m \in T$. Since x_t is the leftmost of the elements of T, x_m is to the right of x_t and, by our choice of x_{k+1}'s location, x_m is to the right of x_{k+1}.

By contraposition, we find that if x_m is to the left of x_{k+1}, then $x_{k+1} \not\leq x_m$. So, our ordered list of V_{k+1} has the desired properties, and, by the principle of mathematical induction, we find that we may create such an ordered list of a partially ordered set of any size. Actually, a permutation that places the elements of a partially ordered set so that $x_i \leq x_j$ implies that x_i falls to the left of x_j is called a *linear extension* of the partially ordered set.

□

2 Compatible Matrices

In our later proof of Möbius inversion, we will make use of what are called *compatible* matrices and several of their properties. We will begin our discussion of compatible matrices with their definition. Note that a matrix is said to be compatible in relation to a specific partially ordered set.

2.1 Definition and Example

Definition 2.1. An $n \times n$ matrix A is *compatible* with respect to the partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$, if $A_{ij} \neq 0$ implies that $x_i \leq x_j$.

For example, consider the partially ordered set $(V, \subseteq)$, where $V = \mathcal{P}(\{a, b, c\})$ (see Figure 1). Define the following:

$x_1 = \emptyset$ $\quad$ $x_3 = \{b\}$ $\quad$ $x_5 = \{a, b\}$ $\quad$ $x_7 = \{b, c\}$

$x_2 = \{a\}$ $\quad$ $x_4 = \{c\}$ $\quad$ $x_6 = \{a, c\}$ $\quad$ $x_8 = \{a, b, c\}$

Then, the reader may verify that the following are all compatible matrices relative to the partially ordered set $(V, \subseteq)$, with the last of the three having a 1 in every entry that may be nonzero (we will later define this particular matrix as the "complete" compatible matrix of $(V, \subseteq)$):

$$\begin{bmatrix} 6 & 0 & 0 & e & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0.65 & 0 & 6 & 0 & 0 & 500 \\ 0 & 0 & 0 & 0 & 3 & \pi & 0 & 1 \\ 0 & 0 & 20 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We may note that the 8×8 matrix comprised of all zeros is also compatible with respect to $(V, \subseteq)$. That the zero matrix satisfies the necessary conditions for being compatible in reference to any partially ordered set is clear.

2.2 Several Properties

From the properties of a partial ordering relation, several properties of compatible matrices are immediately evident. First, note that if A_{ij} (the ijth entry of the matrix A) is nonzero for distinct i and j, then $A_{ji} = 0$. This follows directly from the antisymmetric property established in Definition 1.1. Furthermore, A_{ii} may always be nonzero, and if A_{ij} and A_{jk} are nonzero, then A_{ik} may be nonzero. In these cases, we are using the reflexive and transitive properties, respectively, of Definition 1.1.

Some other, perhaps less obvious, properties of compatible matrices follow.

Theorem 2.1. *Let A and B be $n \times n$ matrices that are compatible with respect to the partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$, and $\leq$ is a partial ordering relation on V. Then $A + B = C$ is also compatible with respect to $(V, \leq)$.*

Proof. Consider two $n \times n$ matrices, A and B, which are compatible with respect to the partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$, and $\leq$ is a partial ordering relation on V.

Because A is compatible, if A_{ij} is nonzero for positive integers i and j less than or equal to n, then $x_i \leq x_j$. Since B is also compatible, B_{ij} can be either nonzero or zero. Then, $A_{ij} + B_{ij}$ is nonzero or zero (the latter is the case in which $A_{ij} = -B_{ij}$) and the property "$C_{ij} \neq 0$ implies $x_i \leq x_j$" is preserved in such entries of the matrix $C = A + B$. Note that the same argument can be made for the case in which B_{ij} is nonzero and A_{ij} is zero.

In the case in which both A_{ij} and B_{ij} are zero, $C_{ij} = A_{ij} + B_{ij} = 0 + 0 = 0$, and so the conditional statement "$C_{ij} \neq 0$ implies $x_i \leq x_j$" is certainly preserved in such entries of the matrix $C = A + B$.

Thus, by definition, if A and B are compatible matrices with respect to $(V, \leq)$, $C = A + B$ is also compatible with respect to $(V, \leq)$.

□

Before we state and prove the next property of compatible matrices, it is important to first note that we may multiply two $n \times n$ matrices using the standard method of matrix multiplication.

Theorem 2.2. *If A and B are $n \times n$ matrices that are compatible with respect to the partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$ and $\leq$ is a partial ordering relation on V, then their product, AB, is also compatible with respect to $(V, \leq)$.*

Proof. Consider a partially ordered set $(V, \leq)$ with $V = \{x_1, x_2, \ldots, x_n\}$, and take $n \times n$ matrices A and B that are compatible with respect to $(V, \leq)$. Let $C = AB$.

To show that C is also compatible with respect to $(V, \leq)$, we must prove that if C_{ij} is nonzero for positive integers i and j less than or equal to n, then $x_i \leq x_j$. If this is the case, A_{ij} must have been nonzero or what I will call a "secret zero," which will denote an entry A_{ij} that is zero while $x_i \leq x_j$. (Recall that our definition for compatible matrices is not a biconditional.)

We find that, for C to be compatible, it is necesssary and sufficient to show that the following is satisfied: if C_{ij} is nonzero, then A_{ij} is either nonzero or a "secret zero".

(Note that this is equivalent to the statement: if C_{ij} is nonzero, then B_{ij} is either nonzero or a "secret zero".)

Suppose that C_{ij} is nonzero, and recall that $C_{ij} = A_{i1}B_{1j} + A_{i2}B_{2j} + \ldots + A_{in}B_{nj}$.

Then, it is clear that at least one of the terms in this sum must be nonzero. Call this term $A_{ik}B_{kj}$. If the product of A_{ik} and B_{kj} is nonzero, then each is separately nonzero and we have the following relations: $x_i \leq x_k$ and $x_k \leq x_j$.

Because our partial ordering relation is, by definition, transitive, we find that $x_i \leq x_j$, and so A_{ij} is either nonzero or a "secret zero".

Therefore, if C_{ij} is nonzero, then A_{ij} is either nonzero or a "secret zero," and we are done. $\square$

2.3 Groundwork for the Final Property

The next property of compatible matrices is in no way self-evident. It states that if the inverse of a compatible matrix exists, then it is also compatible. However, we do not yet have the tools necessary to prove this property, and so will need to work up to its statement and proof.

Consider a matrix A that is compatible with respect to the partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$. From our findings in Section 1.2, we know that we may order the elements of V such that for any pair x_i and x_j where x_i falls to the left of x_j in our list, $x_j \not\leq x_i$.

For the sake of notation, let this list be: $y_1, y_2, \ldots, y_n$, where y_1 is the element of V that is farthest to the left in this list, y_2 is second from the left, etc. up to y_n, which is the rightmost element of V in our ordered list. So if, for example, the beginning of our ordered listing of x's is $x_7, x_4, x_2, x_{13}, \ldots$, then, $y_1 = x_7, y_2 = x_4, y_3 = x_2, y_4 = x_{13}$, etc.

If we think of a compatible matrix as an $n \times n$ matrix whose rows and columns are labeled $x_1, x_2, \ldots, x_n$, we may also consider the matrix whose rows and columns are labeled by $y_1, y_2, \ldots, y_n$. It then becomes clear that another important concept in our discussion will be that of a permutation matrix, which is simply the $n \times n$ identity matrix with its rows reordered so that, when multiplied by any other $n \times n$ matrix on the left or right, it reorders that matrix's rows or columns, respectively. Note that in discussing permutation matrices, we are moving outside of the realm of compatible matrices: that is, a given permutation matrix is not necessarily compatible.

So, using two permutation matrices, we may reorder the rows *and* columns of A so that it is a compatible matrix corresponding to the relationship between the y's rather than the x's. Call this matrix T.

In order to define these permutation matrices more explicitly, recall that:

Definition 2.2. [4, p.114] Given an $m \times n$ matrix A, the *transpose* of A is the $n \times m$ matrix, denoted by A^T, whose columns are formed from the corresponding rows of A.

We say that $T = PAQ$ for permutation matrices P and Q; P is defined as a permutation matrix where P_{ij} is 1 if x_j is in the ith position in our ordered listing of V. Otherwise, P_{ij} is zero. Q is simply the transpose of P. To illustrate this concept, consider the following example:

Example 2.1. *Suppose our ordered listing of* $\{x_1, x_2, x_3, x_4\}$ *is* $[x_1, x_4, x_2, x_3]$. *Then our permutation matrix* P *would be:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Multiplied on the left, this matrix will take a compatible matrix, B, of the partially ordered set defined on the set $\{x_1, x_2, x_3, x_4\}$, and will reorder its rows so that the first row of B becomes the first row of B', the second row of B becomes the third row of B', the third row of B becomes the fourth row of B', and the fourth row of B becomes the second row of B'.

Q, then, is the transpose of P:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Q will rearrange the columns of B' in a similar fashion in order to create T_B.

It is not too difficult to see that T will always be an upper triangular matrix. Consider the entry T_{ij}. If i is greater than j (in the traditional sense of ordered integers), then T_{ij} must be zero by Definition 2.1, since, by our creation of the y's as an ordered listing of the x's, we have established that $y_i \not\leq y_j$.

We have concluded that, given a matrix that is compatible with respect to a partially ordered set $(V, \leq)$, where $V = \{x_1, x_2, \ldots, x_n\}$, we may create a corresponding upper triangular matrix, T, that is compatible with respect to the partially ordered set $(V\star, \leq)$, where $V\star = \{y_1, y_2, \ldots, y_n\}$ is comprised of the elements of V relisted so that if $x_m \leq x_n$, then x_m falls to the left of x_n on our list. For notational simplicity, we then re-label the x's as y's, in sequential order. Note that if the inverse of T is compatible with respect to $V\star$, then the inverse of our original matrix A is compatible with respect to V.

Recall the following properties of matrices:

Theorem 2.3. *If A is a triangular matrix, then* $\det A$ *is the product of the entries on the main diagonal of A.*

Theorem 2.4. *A square matrix A is invertible if and only if* $\det A \neq 0$.

Definition 2.3. The $n \times n$ *identity matrix* is the matrix with 1's on the diagonal and 0's elsewhere.

So, T is invertible if and only if the entries on its main diagonal are all nonzero. It will also be helpful to be aware of a few additional properties of T^{-1} before we begin to work with it in earnest:

- T^{-1} is an upper triangular matrix. To see that this is true, consider deriving T^{-1} by row reducing the augmented matrix $[T\ I]$. If T^{-1}, exists, $[T\ I]$ is row equivalent to $[I\ T^{-1}]$ [4, p.124]. Since T is upper triangular, to reduce T to I, for each given row we need only subtract rows that fall below that given row. When we consider what is happening to I, on the right, while we do this, we see that I only gains entries above the diagonal as it becomes T^{-1}.

- The entries on the main diagonal of T^{-1} are all nonzero. Recall that an $n \times n$ matrix is invertible if and only if its determinant is nonzero, and that the determinant of an upper triangular matrix is the product of the entries on its main diagonal. Then, if any of the entries on the diagonal of T^{-1} were zero, T^{-1} would not be invertible. However, T^{-1} is clearly invertible, as it is the inverse of T.

So, all entries T^{-1}_{ij} where $i > j$ are equal to zero, and all entries T^{-1}_{jj} are nonzero. We can see that both properties are allowed in a compatible matrix. So, in our proof that T^{-1} is compatible, we need only look at entries T^{-1}_{ij} of T^{-1} where $i < j$, and ensure that if $T^{-1}_{ij} \neq 0$, then $y_i \leq y_j$.

2.4 The Final Property

Now, we may move on to the final property of compatible matrices that we will explore in this paper.

Theorem 2.5. *If the inverse of an upper triangular matrix T that is compatible with respect to the partially ordered set $(V\star, \leq)$ exists, then T^{-1} is also compatible with respect to $(V\star, \leq)$.*

Proof. We will use the principle of strong induction to show that for all entries that lie above the diagonal in the jth (where $2 \leq j \leq n$) column of an $n \times n$ matrix T^{-1} (where T^{-1} is the inverse of a compatible upper triangular matrix T), the following property holds:

$$\text{If the entry } T^{-1}_{ij} \text{ is nonzero, then } y_i \leq y_j.$$

In other words, we will prove that T^{-1} is a compatible matrix by considering the entries $T^{-1}_{(j-k)j}$ for $1 \leq k \leq (j-1)$. In particular, in each step of our induction on k, we will prove that $T^{-1}_{(j-k)j} \neq 0 \Rightarrow y_i \leq y_j$ by contraposition.

As our base case, let $k = 1$ and suppose $y_{j-1} \not\leq y_j$. Then we are considering the entry $T^{-1}_{(j-1)j}$.

Recall that $TT^{-1} = I(= T^{-1}T)$, where I is the $n \times n$ identity matrix. The $(j-1)j$th entry of I is equal to zero by definition, and so, from standard matrix multiplication,

$$T_{(j-1)1}T^{-1}_{1j} + T_{(j-1)2}T^{-1}_{2j} + \ldots + T_{(j-1)(j-1)}T^{-1}_{(j-1)j} + T_{(j-1)j}T^{-1}_{jj} + \ldots + T_{(j-1)n}T^{-1}_{nj} = 0. \qquad (1)$$

However, because T and T^{-1} are both upper triangular matrices, we see that $T_{(j-1)1}, T_{(j-1)2}, T_{(j-1)2}, \ldots,$ $T_{(j-1)(j-2)}$ and $T^{-1}_{(j+1)j}, T^{-1}_{(j+2)j}, T^{-1}_{(j+3)j}, \ldots, T^{-1}_{nj}$ are all equal to zero. So, our sum on the left in equation (1) reduces to

$$T_{(j-1)(j-1)}T^{-1}_{(j-1)j} + T_{(j-1)j}T^{-1}_{jj} = 0.$$

Since T is a compatible matrix and $y_{j-1} \not\leq y_j$, we see that $T_{(j-1)j} = 0$ by definition. Then, we have

$$T_{(j-1)(j-1)}T^{-1}_{(j-1)j} = 0.$$

Because T is an invertible upper triangular matrix, and $T_{(j-1)(j-1)}$ is an entry on its diagonal, $T_{(j-1)(j-1)}$ is nonzero. Then, $T^{-1}_{(j-1)j}$ must be equal to zero. We have now shown that, for $k = 1$, if $y_{j-k} \not\leq y_j$, then $b_{(j-k)j} = 0$. By contraposition, if $b_{(j-k)j} \neq 0$, then $y_{j-k} \leq y_j$.

Next, suppose this holds true for all k up to $k = l - 1$. Thus, if $T^{-1}_{(j-k)j} \neq 0$ for $1 \leq k \leq (l-1)$, then $y_{j-k} \leq y_j$.

Suppose $y_{j-l} \not\leq y_j$. We will look at the $(j-l)j$th entry of the identity matrix. This entry will be equal to zero, since $(j-l) \neq j$. From the product of T and T^{-1}, it is clear that the following equation holds

$$T_{(j-l)1}T^{-1}_{1j} + T_{(j-l)2}T^{-1}_{2j} + \ldots + T_{(j-l)(j-l)}T^{-1}_{(j-l)j} + \ldots + T_{(j-l)j}T^{-1}_{jj} + \ldots + T_{(j-l)n}T^{-1}_{nj} = 0.$$

As was the case before, this reduces down to

$$T_{(j-l)(j-l)}T^{-1}_{(j-l)j} + T_{(j-l)(j-l+1)}T^{-1}_{(j-l+1)j} + \ldots + T_{(j-l)j}T^{-1}_{jj} = 0.$$

Since T is a compatible matrix and $y_{j-l} \not\leq y_j$, we see that $T_{(j-l)j} = 0$. Then:

$$T_{(j-l)(j-l)}T^{-1}_{(j-l)j} + T_{(j-l)(j-l+1)}T^{-1}_{(j-l+1)j} + \ldots + T_{(j-l)(j-1)}T^{-1}_{(j-1)j} = 0. \tag{2}$$

Suppose, by way of contradiction, that $T_{(j-l)(j-l)}T^{-1}_{(j-l)j} \neq 0$. Then, in order for equation (2) to hold, it must be the case that $T_{(j-l)(j-l+1)}T^{-1}_{(j-l+1)j} + \ldots + T_{(j-l)(j-1)}T^{-1}_{(j-1)j} \neq 0$. Clearly, at least one of the terms must be nonzero. Without loss of generality, call this nonzero term $T_{(j-l)t}T^{-1}_{tj}$, where $(j-l+1) \leq t \leq (j-1)$. Note that $t = j - m$ for $1 \leq m \leq (l-1)$ and that $T_{(j-l)t}$ and T^{-1}_{tj} are both nonzero. From our induction step, we know that if T^{-1}_{tj} is nonzero, then $y_t \leq y_j$. T is compatible relative to $(V\star, \leq)$, and so $T_{(j-l)t} \neq 0$ implies that $y_{j-l} \leq y_t$. Because our partial ordering relation is transitive, we see that:

$$y_{j-l} \leq y_t \wedge y_t \leq y_j \Rightarrow y_{j-l} \leq y_j \ .$$

However, this contradicts our assumption that $y_{j-l} \not\leq y_j$. Then what we assumed is false, and $T_{(j-l)(j-l)}T^{-1}_{(j-l)j} = 0$. We know that $T_{(j-l)(j-l)} \neq 0$, since it is an entry on the diagonal of T, so we conclude that $T^{-1}_{(j-l)j} = 0$. In summary, $y_{j-l} \not\leq y_j$ implies that $T^{-1}_{(j-l)j} = 0$, and so, by contraposition, $T^{-1}_{(j-l)j} \neq 0$ implies that $y_{j-l} \leq y_j$.

We have shown that the statement "if $T^{-1}_{(j-k)j} \neq 0$, then $y_{j-k} \leq y_j$" holds for $k = 1$, and that if it holds for all k up to $k = l - 1$ then it holds for $k = l$. Thus, by the principle of strong induction, "if $T^{-1}_{(j-k)j} \neq 0$, then $y_{j-k} \leq y_j$" holds for all positive integers k. Note, however, that this does not make sense for $k > (j - 1)$, so we limit our conclusion to encompass only the integers k such that $1 \leq k \leq (j - 1)$.

Finally, recall that our choice of column j was completely arbitrary. Thus, we have effectively shown that if any entry T^{-1}_{ij} that lies above the main diagonal is nonzero, then $y_i \leq y_j$. This is sufficient to show that T^{-1} is compatible with respect to the partially ordered set $(V\star, \leq)$.

□

As mentioned earlier, this implies that the inverse of our original matrix A, from which T was derived, is compatible with respect to $(V, \leq)$. So, we have shown the following:

Theorem 2.6. *If the inverse of a matrix A that is compatible with respect to the partially ordered set $(V, \leq)$ exists, then A^{-1} is also compatible with respect to $(V, \leq)$.*

2.5 Complete Compatible Matrices

Earlier, we mentioned that there are infinitely many matrices that are compatible with respect to a given partially ordered set $(V, \leq)$. In order to take away the most information about a partially ordered set from one of its compatible matrices, we would like that matrix to have a nonzero entry in each position it is allowed to have a nonzero entry by definition. The concept of a complete compatible matrix addresses this desire by defining a particular (and quite tidy) "ideal" compatible matrix of $(V, \leq)$.

Definition 2.4. A matrix Z, which is compatible with respect to the partially ordered set $(V, \leq)$, is said to be the *complete compatible* matrix of $(V, \leq)$ when

$$Z_{ij} = \begin{cases} 1 & \text{if } x_i \leq x_j, \\ 0 & \text{otherwise,} \end{cases}$$

where x_i, $x_j \in V = \{x_1, x_2, \ldots, x_n\}$.

Note that the complete compatible matrix of a given partially ordered set is unique up to the labeling of the elements. For example, we may use permutation matrices to create a matrix that

is the complete compatible matrix with respect to any linear extension of a given partially ordered set (See the Section 2.3). This complete compatible matrix is not necessarily equal to the complete compatible matrix generated by the original labeling of the partially ordered set. However, assuming a fixed labeling of the elements of our partially ordered set, its corresponding complete compatible matrix is, indeed, unique.

In considering M, the inverse of a complete compatible matrix Z, we note that, if M exists, then it is also compatible with respect to $(V, \leq)$ (see Theorem 2.5). In fact, M always exists, which brings us to the following result:

Theorem 2.7. *If Z is the complete compatible matrix of a partially ordered set $(V, \leq)$, then $Z^{-1} = M$ exists.*

Proof. For a given partially ordered set, we may label the elements of the set in any way we choose. Specifically, label the elements such that if $x_m \leq x_n$, then $m \leq n$. Then, Z is an upper triangular matrix (see Sections 1.2 and 2.3), and all diagonal entries of Z are equal to 1 by definition. Since the determinant of an upper triangular matrix is the product of its diagonal entries by Theorem 2.3 (in the case of the complete compatible matrix, $\det Z = 1$), and an $n \times n$ matrix is invertible if and only if its determinant is nonzero by Theorem 2.4, we find that Z is invertible. Therefore, $Z^{-1} = M$ exists. □

3 The Möbius Function

In order to work up to the concept of Möbius inversion, we must first define what is known as the Möbius function. In this section, we will state the definition of the Möbius function, prove its existence, and explicitly define the function in the context of several common structures of partially ordered sets. These last definitions will be useful as we begin to look at applications of the Möbius inversion formula in later sections.

Definition 3.1. [6] The Möbius function μ is defined on $(V, \leq) \times (V, \leq)$ by the following properties for x_i, x_j, $x_k \in V$:

$$\mu(x_i, x_j) = 0 \text{ if } x_i \not\leq x_j \ ,$$
$$\mu(x_i, x_i) = 1 \ ,$$
$$\sum_{x_i \leq x_j \leq x_k} \mu(x_i, x_j) = 0 \text{ if } x_i < x_k \ .$$

(Note that "$x_i < x_k$" is defined as "$x_i \leq x_k$ and $x_i \neq x_k$.")

3.1 Establishing Existence

We will show that $\mu(x_i, x_j) = M_{ij}$, where M is the inverse of the complete compatible matrix Z of $(V, \leq)$, satisfies each of these properties and so is, by definition, the Möbius function.

Lemma 3.1. *$M_{ij} = 0$ if $x_i \not\leq x_j$.*

Proof. As was previously noted, M, as the inverse of the compatible matrix Z, is also compatible with respect to $(V, \leq)$ (see Theorem 2.5). By the definition of a compatible matrix (see Definition 2.1), if $M_{ij} \neq 0$, then $x_i \leq x_j$. By the contrapositive of this conditional statement, if $x_i \not\leq x_j$, then $M_{ij} = 0$. □

We will review several results from linear algebra before we show the validity of the next property of the Möbius function.

Definition 3.2. [4, p.187] For any square matrix A, let $\tilde{A}_{ij}$ denote the submatrix formed by deleting the ith row and jth column of A.

Definition 3.3. [4, p.203] The *adjugate*, or *classical adjoint*, of a matrix A is denoted by adj$A$, and is given by:

$$\begin{bmatrix} C_{11} & \dots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \dots & C_{nn} \end{bmatrix},$$

Where $C_{ij} = (-1)^{i+j} \det \tilde{A}_{ij}$.

Theorem 3.1. [4, p.203] *Let A be an invertible $n \times n$ matrix. Then*

$$A^{-1} = \frac{1}{\det A} \text{adj} A \ .$$

Now we may move on to a proof that the second property of the Möbius function holds for $\mu(x_i, x_j) = M_{ij}$.

Lemma 3.2. *$M_{ii} = 1$.*

Proof. By Theorem 3.1, $Z^{-1} = \frac{1}{\det Z} \text{adj} Z$ where 'adj' denotes the adjugate of Z. So,

$$Z^{-1} = \frac{1}{\det Z} \begin{bmatrix} C_{11} & \dots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \dots & C_{nn} \end{bmatrix},$$

where $C_{ij} = (-1)^{i+j} \det \tilde{Z}_{ij}$.

Since $\det Z = 1$,

$$Z^{-1} = \begin{bmatrix} C_{11} & \dots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \dots & C_{nn} \end{bmatrix},$$

So, $M_{ii} = C_{ii} = (-1)^{2i} \det \tilde{Z}_{ii} = \det \tilde{Z}_{ii}$.

Note that $\det \tilde{Z}_{ii} = 1$, since $\tilde{Z}_{ii}$ is simply the matrix Z defined on $(V \setminus \{x_i\}, \leq)$, and all arguments we have made regarding the determinant apply to the matrix Z regardless of the size of the partially ordered set from which Z is formed.

Therefore, $M_{ii} = 1$. □

Lemma 3.3.

$$\sum_{x_i \leq x_j \leq x_k} M_{ij} = 0 \text{ if } x_i < x_k \ .$$

Proof. Since $MZ = I$, where I is the $n \times n$ identity matrix, we see that for $x_i < x_k$ (and thus $i \neq k$),

$$M_{i1}Z_{1k} + M_{i2}Z_{2k} + \ldots + M_{in}Z_{nk} = I_{ik} = 0.$$

Since Z is compatible, the only Z_{jk}'s that will be nonzero are those for which $x_j \leq x_k$. Furthermore, these entries will be equal to 1 by the definition of Z. Then, our sum reduces to a sum of all M_{ij}'s where $x_j \leq x_k$. Note that, because M is also compatible, the only terms of this simplified sum that will be nonzero are those for which $x_i \leq x_j$. In summary,

$$\sum_{x_i \leq x_j \leq x_k} M_{ij} = 0.$$

□

Therefore, because $\mu(x_i, x_j) = M_{ij}$ satifies the necessary and sufficient properties outlined in Definition 3.1, it is a representation of the Möbius function. Now that we have proven its existence, we will prove the uniqueness of the Möbius function. Note that M is unique up to the labeling of the elements of the partially ordered set (See Section 2.5 for further discussion of uniqueness). As we develop our proof, we will assume a fixed labeling. Regardless of how we label, however, the Möbius function's uniqueness holds: we are claiming that specific entries of M define the Möbius function, not the structure of M itself.

3.2 Establishing Uniqueness

Lemma 3.4. *The Möbius function is unique.*

Proof. To prove that the Möbius function is unique, consider a function γ defined on $(V, \leq) \times (V, \leq)$, where $V = \{x_1, x_2, x_3, \ldots, x_k\}$, such that γ satisfies all the properties necessary to be deemed the Möbius function. Build a $k \times k$ matrix N such that $N_{ij} = \gamma(i, j)$, and let Z be the complete compatible matrix of $(V, \leq)$. We established in earlier in this section that $Z^{-1} = M$ is the Möbius function. To show the uniqueness of the Möbius function, it is sufficient to show that $N = M$, or, alternatively, that $ZN = I$, where I is the $k \times k$ identity matrix.

To do so, consider the product ZN. We must show that each diagonal entry of this product is equal to 1, and that each entry not on a diagonal is equal to zero.

Consider $(ZN)_{ii}$, an arbitrary diagonal entry of the product. Performing basic matrix multiplication, we find that:

$$(ZN)_{ii} = \sum_{j=1}^{k} Z_{ij} N_{ji} \ .$$

Note that because Z is the complete compatible matrix of $(V, \leq)$, Z_{ij} is nonzero exactly when $x_i \leq x_j$, and that when this is true, $Z_{ij} = 1$. We may, then, simplify our sum:

$$(ZN)_{ii} = \sum_{1 \leq j \leq k,\ x_i \leq x_j} N_{ji} \ .$$

However, by the first property of the Möbius function (see Definition 3.1), $N_{ji} = 0$ when $x_j \not\leq x_i$. Thus, the only nonzero term of our sum is N_{ii}, which, from the second property of the Möbius function, is equal to 1. So, $(ZN)_{ii} = 1$.

Next, consider an entry $(ZN)_{il}$ of the matrix ZN, where $i \neq l$. As before, we may rewrite this entry in summation notation:

$$(ZN)_{il} = \sum_{j=1}^{k} Z_{ij} N_{jl} \ . \tag{3}$$

As in the first case, note that $Z_{ij} = 1$ when $x_i \leq x_j$, and is equal to zero otherwise. Then, rewriting again:

$$(ZN)_{il} = \sum_{1 \leq j \leq k,\ x_i \leq x_j} N_{jl} \ .$$

By our definition of N, the only nonzero terms of this sum are those j's for which $x_j \leq x_l$. Then,

$$(ZN)_{il} = \sum_{x_i \leq x_j \leq x_l} N_{jl} = \sum_{x_i \leq x_j \leq x_l} \mu(j,l) \ .$$

By the third property of the Möbius function, $(ZN)_{il} = 0$ when $x_i < x_l$. (Note that if $x_i \not< x_l$, either $x_i \not< x_j$ or $x_j \not< x_l$ for each $1 \leq j \leq k$ since the partial ordering relation is transitive, and so the terms of Equation 3 are all equal to zero, and thus the entire sum is equal to zero.)

Thus, we have shown that $ZN = I$, or $N = M$, and so the Möbius function is unique.

□

3.3 Several Examples

Next, we will look at partially ordered sets that are made up of the subsets of a set paired with the partial ordering relation $\subseteq$, and the divisors of a positive integer paired with the partial ordering relation "divides" ($|$). By looking at several specific examples, we will develop the general form of the Möbius function for similarly constructed partially ordered sets.

3.3.1 Sets

Our first example will be the partially ordered set consisting of all subsets of the set $\{a, b, c\}$ together with the partially ordering relation $\subseteq$. Recall that we discussed this particular partially ordered set in Section 1.1. We will refer to the Hasse diagram in that section throughout this example.

Example 3.1. The relationships between elements of the partially ordered set V defined by $\mathcal{P}(\{a, b, c\}), \subseteq$ may be seen in its corresponding Hasse diagram (Figure 1).

Building the Möbius function of this poset from the ground up, we first note that, by definition, if $A \nsubseteq B$ for A, $B \in S$, then $\mu(A, B) = 0$. Furthermore, $\mu(A, A) = 1$ for each $A \in V$.

We will start by looking at any two elements A and B that are consecutive in Figure 1. By consecutive, we mean to say that two elements are directly connected by a single line segment. For example, $\{a\}$ and $\{a, b\}$ are consecutive elements, while $\{a\}$ and $\{a, b, c\}$ are not. By the third property of the Möbius function (see Definition 3.1),

$$\sum_{A \subseteq X \subseteq B} \mu(A, X) = 0.$$

However, because A and B are consecutive, there are no elements of the poset that are strictly "between" them. So we find that:

$$\sum_{A \subseteq X \subseteq B} \mu(A, X) = \mu(A, A) + \mu(A, B) = 0. \tag{4}$$

As discussed, $\mu(A, A) = 1$. Then, it is clear that:

$$\mu(A, B) = -1.$$

This argument takes care of much of our work:

$\mu(\emptyset, \{a\}) = \mu(\emptyset, \{b\}) = \mu(\emptyset, \{c\}) = -1$
$\mu(\{a\}, \{a, b\}) = \mu(\{a\}, \{a, c\}) = -1$
$\mu(\{b\}, \{a, b\}) = \mu(\{b\}, \{b, c\}) = -1$
$\mu(\{c\}, \{a, c\}) = \mu(\{c\}, \{b, c\}) = -1$

and,

$\mu(\{a, b\}, \{a, b, c\}) = \mu(\{a, c\}, \{a, b, c\}) = \mu(\{b, c\}, \{a, b, c\}) = -1.$

The only μ's we have left to define are $\mu(\emptyset, \{a, b\})$, $\mu(\emptyset, \{a, c\})$, $\mu(\emptyset, \{b, c\})$, $\mu(\emptyset, \{a, b, c\})$, $\mu(\{a\}, \{a, b, c\})$, $\mu(\{b\}, \{a, b, c\})$, and $\mu(\{c\}, \{a, b, c\})$.

Again using the third property of the Möbius function, we find that this is relatively straightforward:

$$\sum_{\{a\} \subseteq X \subseteq \{a,b,c\}} \mu(\{a\}, X) = \mu(\{a\}, \{a\}) + \mu(\{a\}, \{a, b\}) + \mu(\{a\}, \{a, c\}) + \mu(\{a\}, \{a, b, c\}) = 0. \tag{5}$$

So, $1 - 1 - 1 + \mu(\{a\}, \{a, b, c\}) = 0$, and $\mu(\{a\}, \{a, b, c\}) = 1$.

By similar arguments,

$\mu(\{b\}, \{a, b, c\}) = \mu(\{c\}, \{a, b, c\}) = \mu(\emptyset, \{a, b\}) = \mu(\emptyset, \{a, c\}) = \mu(\emptyset, \{b, c\}) = 1,$

and,

$\mu(\emptyset, \{a, b, c\}) = -1.$

We have thus explicitly defined the Möbius function for all elements of $(V, \subseteq) \times (V, \subseteq)$.

Generalizing our results, we arrive at the following:

Theorem 3.2. *Suppose A and B are elements of the partially ordered set defined by $\mathcal{P}(S)$ for some set S and the partial ordering relation $\subseteq$, such that $A \subseteq B$. Then, $\mu(A, B) = (-1)^{|B|-|A|}$.*

Proof. Suppose A and B are elements of the partially ordered set defined by $\mathcal{P}(S)$ for some set S and the partial ordering relation $\subseteq$, such that $A \subseteq B$. We will prove Theorem 3.2 using the principle of strong induction on $k = |B| - |A|$.

As our base case, suppose $k = 0$. Then, $|B| = |A|$. Since $A \subseteq B$, we find that $A = B$.

By definition, $\mu(A, B) = \mu(A, A) = 1 = (-1)^0 = (-1)^{|B|-|A|}$, and we have shown that Theorem 3.2 holds for $k = 0$.

Suppose $k = 1$. Then, $B = A \cup \{b_1\}$ for some b_1 not in A. So, A and B are consecutive subsets, and we know from a generalization of our argument in Example 3.1 (specifically, Equation 4) that $\mu(A, B) = -1 = (-1)^1 = (-1)^{|B|-|A|}$. So, Theorem 3.2 holds for $k = 1$.

Suppose Theorem 3.2 holds for all k up to $k = n - 1$. Consider the case in which $k = n$.

We note that $B = \{b_1, b_2, \ldots, b_n\} \cup A$, where $b_1, b_2, \ldots, b_n$ are distinct and are not elements of A.

Note that we may remove b_1, b_2, ..., b_{n-1}, or b_n from the set B to produce the subsets $\{b_2, b_3, \ldots, b_n\} \cup A$, $\{b_1, b_3, \ldots, b_n\} \cup A$, ..., $\{b_1, b_2, \ldots, b_{n-2}, b_n\} \cup A$, and $\{b_1, b_2, \ldots, b_{n-1}\} \cup A$. Thus, there are $\binom{n}{1}$ subsets of B of order $(n-1) + |A|$. Note that, by our induction hypothesis, $\mu(A, C)$, where C is one of these subsets, is equal to $(-1)^{|C|-|A|}$.

Similarly, there are $\binom{n}{2}$ subsets of order $(n-2) + |A|$, etc, all the way down to $\binom{n}{n-1}$ subsets of order $(1) + |A|$, and finally, $\binom{n}{n} = 1$ subset of order $|A|$ (namely, A itself).

Then, from the third property of the Möbius function, and because Theorem 3.2 holds for all k up to $k = n - 1$,

$$\sum_{A \subseteq S \subseteq B} \mu(A, S) = \binom{n}{1}(-1)^{n-1} + \binom{n}{2}(-1)^{n-2} + \ldots + \binom{n}{n-1}(-1)^1 + \binom{n}{n}(-1)^0 + \mu(A, B) = 0.$$

Simplifying and rearranging, we see that:

$$\sum_{j=1}^{n} \binom{n}{j}(-1)^{n-j} + \mu(A, B) = \sum_{j=0}^{n} \binom{n}{j}(-1)^{n-j} - \binom{n}{0}(-1)^n + \mu(A, B) = 0.$$

By noticing that the sum may be rewritten using the binomial theorem, we see that:

$$(1-1)^n - \binom{n}{0}(-1)^n + \mu(A, B) = 0 - \binom{n}{0}(-1)^n + \mu(A, B) = 0.$$

And so, $\binom{n}{0}(-1)^n = (-1)^n = (-1)^{|B|-|A|} = \mu(A, B)$, and we have shown that Theorem 3.2 holds

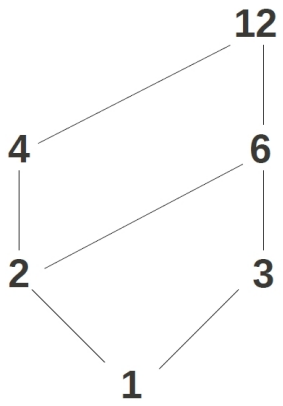

Figure 2: The Hasse diagram for the partially ordered set $(V, |)$, where V is the set of all divisors of 12.

for $k = n$.

Thus, by the principle of strong induction, Theorem 3.2 holds for all positive integers k and thus $\mu(A, B) = (-1)^{|B|-|A|}$ for all sets A and B such that $A \subseteq B$.

□

3.3.2 Divisors

Our definition of the Möbius function in the case of a partially ordered set made up of the divisors of an integer and the partial ordering relation "divides" is similar to the definition for the subsets case. Consider that, by the fundamental theorem of arithmetic, we may express any integer greater than 1 uniquely as a product of primes. So, we may express each integer in our partially ordered set as a set made up of its prime divisors. For example, $14 = 2 \times 7$ would be expressed as $\{2, 7\}$. Note, however, that these primes are not necessarily distinct, and so we may have multisets such as $\{2, 2, 2\}$, which is the set form of $8 = 2 \times 2 \times 2$, and is not the same as $\{2, 2\}$ or $\{2\}$, which are the set forms of $4 = 2 \times 2$ and $2 = 2$, respectively. It is clear, then, that we must revise Theorem 3.2 in some way in order to apply it to this new partially ordered set.

First, consider as an example the integer 12 and its prime divisors together with the partial ordering relation "divides."

Example 3.2. The Hasse diagram of the partially ordered set defined by the set of divisors of 12 and the partial ordering relation "divides" is shown in Figure 2.

As was the case in Example 3.1, if d is a divisor of 12, then $\mu(d, d) = 1$. Also as in our previous

example, we see that for two "consecutive" divisors d_1 and d_2 of 12, $\mu(d_1, d_2) = -1$. Thus,

$$\mu(1,3) = \mu(1,2) = \mu(2,4) = \mu(2,6) = \mu(3,6) = \mu(4,12) = \mu(6,12) = -1.$$

What remains to be defined are the following: $\mu(1,4)$, $\mu(1,6)$, $\mu(1,12)$, $\mu(2,12)$, and $\mu(3,12)$.

Note, however, that from the third property of the Möbius function,

$$\sum_{1|d|4} \mu(1,d) = \mu(1,1) + \mu(1,2) + \mu(1,4) = 0,$$

$$\sum_{1|d|6} \mu(1,d) = \mu(1,1) + \mu(1,2) + \mu(1,3) + \mu(1,6) = 0,$$

$$\sum_{1|d|12} \mu(1,d) = \mu(1,1) + \mu(1,2) + \mu(1,3) + \mu(1,4) + \mu(1,6) + \mu(1,12) = 0,$$

$$\sum_{2|d|12} \mu(2,d) = \mu(2,2) + \mu(2,4) + \mu(2,6) + \mu(2,12) = 0,$$

and,

$$\sum_{3|d|12} \mu(3,d) = \mu(3,3) + \mu(3,6) + \mu(3,12) = 0.$$

So, $\mu(1,4) = 0$, $\mu(1,6) = 1$, $\mu(1,12) = 0$, $\mu(2,12) = 1$, and $\mu(3,12) = 0$.

We may state a generalization of our findings:

Theorem 3.3. *Suppose a and b are elements of some partially ordered set defined by the set of divisors of some integer c and the partial ordering relation "divides," such that $a|b$. Then,*

$$\mu(a,b) = \begin{cases} (-1)^k & \text{if } \frac{b}{a} = p_1 p_2 \dots p_k \text{ for distinct primes } p_1, p_2, \dots p_k, \\ 0 & \text{if some prime in the prime decomposition of } \frac{b}{a} \text{ has multiplicity } \geq 2. \end{cases}$$

Proof. Suppose a and b are elements of the partially ordered set as described in Theorem 3.3.

We will prove the theorem using the principle of strong induction on k, the number of (not necessarily distinct) primes in the unique prime factorization of the quotient $\frac{b}{a}$.

Suppose, first, that $k = 0$. Then there are no primes in the quotient $\frac{b}{a}$. In other words, $b = a$. Then, by our definition of the Möbius function, $\mu(a, b) = \mu(a, a) = 1 = (-1)^0$. Thus, we have shown that the proposition holds for $k = 0$.

Next, consider the case where $k = 1$. Then $b = ap$ for some prime p. By the third property of the Möbius function (see Definition 3.1),

$$\sum_{a|d|b} \mu(a, d) = \mu(a, a) + \mu(a, b) = 1 + \mu(a, b) = 0,$$

so $\mu(a, b) = -1 = (-1)^1$, which proves Theorem 3.3 for $k = 1$.

Suppose $k = 2$. Here, we begin to see the reasoning behind the extra caveat of Theorem 3.3. When $k = 2$, we have two cases. Either $b = ap^2$ for some prime p, or $b = apq$ for distinct primes p and q.

In the first case, by the third property of the Möbius function,

$$\sum_{a|d|b} \mu(a, d) = \mu(a, a) + \mu(a, ap) + \mu(a, b) = 1 - 1 + \mu(a, b) = 0,$$

and so $\mu(a, b) = 0$.

In the second case, the same property of the Möbius function yields:

$$\sum_{a|d|b} \mu(a, d) = \mu(a, a) + \mu(a, ap) + \mu(a, aq) + \mu(a, b) = 1 - 1 - 1 + \mu(a, b) = 0,$$

and so $\mu(a, b) = 1 = (-1)^2$. From this and the first case, we have shown that Theorem 3.3 holds for $k = 2$.

Suppose, next, that the proposition holds for $k = (n - 1)$. Consider the case in which $k = n$. Then $b = ap_1p_2 \cdots p_n$ for not necessarily distinct $p_1, p_2, \ldots, p_n$. If $p_1, p_2, \ldots, p_n$ are distinct, then we may simply revert back to our idea of integers as sets and our proof of Theorem 3.2 to show that $\mu(a, b) = (-1)^n$. Suppose, instead, that $p_1, p_2, \ldots, p_n$ are not distinct, and consider $\mu(a, d)$, where $d \neq b$ and $a|d|b$. Since there must be fewer than n primes in the prime decomposition of $\frac{d}{a}$, Theorem 3.3 holds for all $\mu(a, d)$ by our induction hypothesis.

So, we know that if t is a divisor of b such that $t \neq b$ and $\frac{t}{a}$ has a prime divisor with multiplicity greater than 1, $\mu(a, t) = 0$. Otherwise, the divisor of b divides $c = aq_1q_2 \cdots q_m$, where the q_is are exactly the distinct elements of $\{p_1, p_2, \ldots, p_n\}$. Again drawing on the third property of the Möbius function,

$$\sum_{a|d|c} \mu(a, d) = 0.$$

Then,

$$\sum_{a|d|b} \mu(a, d) = \sum_{a|d|c} \mu(a, d) + \sum \mu(a, t) + \mu(a, b) = 0,$$

where c is defined as above and the t's are such that $t \neq b$ and $\frac{t}{a}$ has a prime in its prime decomposition with multiplicity greater than 1. Simplifying,

$$\sum_{a|d|b} \mu(a,d) = \sum_{a|d|c} \mu(a,d) + \sum \mu(a,t) + \mu(a,b) = 0 + 0 + \mu(a,b) = 0.$$

Thus, we have shown that Theorem 3.3 holds for $k = n$, and so, by the principle of strong induction, Theorem 3.3 holds for every possible choice of primes in the prime decomposition of $\frac{b}{a}$, and so holds for all a and b, where a and b are elements of the partially ordered set described in Theorem 3.3, and $a|b$.

□

4 The Möbius Inversion Formula

In Section 3.1, we established that $\mu(x_i, x_j) = M_{ij}$, where M is the inverse of the complete compatible matrix Z, satisfies the properties necessary to be defined as the Möbius function. From this, showing the validity of what is known as the Möbius inversion formula, which is stated below, is straightforward.

4.1 Definition

Theorem 4.1. [6] *Suppose that f is any function on the partially ordered set $(V, \leq)$, x_i and $x_j \in V$, and*

$$g(x_j) = \sum_{x_i \leq x_j} f(x_i) \ .$$

Then,

$$f(x_j) = \sum_{x_i \leq x_j} g(x_i)\mu(x_i, x_j) \ .$$

Proof. Suppose that f is any function on $(V, \leq)$, x_i and $x_j \in V$, and

$$g(x_j) = \sum_{x_i \leq x_j} f(x_i) \ .$$

Let Z be the complete compatible matrix on $(V, \leq)$, and let $M = Z^{-1}$. Since Z_{ij} is equal to 1 exactly when $x_i \leq x_j$, we may rewrite this as:

$$g(x_j) = \text{the } j\text{th entry of the product } \begin{bmatrix} f(x_1) & f(x_2) & \dots & f(x_n) \end{bmatrix} Z$$

Consider the sum:

$$\sum_{x_i \leq x_j} g(x_i)\mu(x_i, x_j) = \sum_{x_i \leq x_j} g(x_i)M_{ij} \ .$$

Since M_{ij} is nonzero only if $x_i \leq x_j$, we may rewrite this as:

$$\text{the } j\text{th entry of the product } \begin{bmatrix} g(x_1) & g(x_2) & \dots & g(x_n) \end{bmatrix} M \ .$$

As we found above, $g(x_i)$ is the ith entry of the $(1 \times n)$ matrix $\begin{bmatrix} f(x_1) & f(x_2) & \dots & f(x_n) \end{bmatrix} Z$. Then, $\sum_{x_i \leq x_j} g(x_i)M_{ij}$= the jth entry of $\begin{bmatrix} f(x_1) & f(x_2) & \dots & f(x_n) \end{bmatrix} ZM$. Since ZM is the $n \times n$ identity matrix, we find that this product is simply $\begin{bmatrix} f(x_1) & f(x_2) & \dots & f(x_n) \end{bmatrix}$. The jth entry, then, is $f(x_j)$. Therefore,

$$\sum_{x_i \leq x_j} g(x_i)M_{ij} = f(x_j) \ ,$$

and we have proven Theorem 4.1.

□

5 The Principle of Inclusion and Exclusion

The combinatorially invaluable principle of inclusion and exclusion is a tool used to indirectly count the number of elements in some universal set that satisfy a given condition. Essentially, we count the number of things that do not satisfy our given condition, and subtract that number from the size of the universal set. Certainly it is sometimes easier to directly count how many things satisfy the condition. However, in many cases, the principle of inclusion and exclusion provides a vastly expedited method. Though the proof of the principle of inclusion and exclusion typically follows a combinatorial argument, we will provide an alternate method of proving its validity using the Möbius inversion formula (see Theorem 4.1).

5.1 A Bit of an Aside

In order to prove the principle of inclusion and exclusion using the Möbius inversion formula, we first must establish several properties of set unions and intersections. While the results of this section are necessary to our later proof of the principle of inclusion and exclusion, their proofs, though interesting in and of themselves, become a bit tedious. The squeamish reader may accept the final result of the section without proof and pass on to Section 5.2.

We will begin by letting $A_1, A_2, \dots, A_j$ be subsets of some set S, and letting $J = \{1, 2, \dots, j\}$.

Lemma 5.1. *Suppose K is a set of positive integers such that $K \subseteq J$. Then,*

$$\bigcap_{i \notin K} A_i = \bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right] .$$

Proof. We will prove equality by showing that the two sets are subsets of one another.

First, let $m \in \bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right]$. Then, $m \in \left[\bigcap_{i \in I_0} A_i^c \cap \bigcap_{i \notin I_0} A_i \right]$ for some $I_0 \subseteq K$ and so $m \in \bigcap_{i \notin I_0} A_i$.

Note that $\bigcap_{i \notin I_0} A_i \subseteq \bigcap_{i \notin K} A_i$. We may see this by noting that if $k \in \bigcap_{i \notin I_0} A_i$, then $k \in A_{k_1}, A_{k_2}, A_{k_3}, \ldots,$ and $A_{k_{|J|-|I_0|}}$, where the k_i's are exactly the elements of the complement of I_0. Some of these k_i's belong to K. Remove these and notice that the A's that remain are exactly those A_i's such that $i \notin K$. Then, $k \in \bigcap_{i \notin K} A_i$.

Therefore, since $m \in \bigcap_{i \notin I_0} A_i$ and $\bigcap_{i \notin I_0} A_i \subseteq \bigcap_{i \notin K} A_i$, it is clear that $m \in \bigcap_{i \notin K} A_i$.

Thus,

$$\bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right] \subseteq \bigcap_{i \notin K} A_i \ . \tag{6}$$

Next, suppose that $m \in \bigcap_{i \notin K} A_i$.

Consider each $i \in K$. If $m \notin A_i$, place i in the set I_0. Otherwise, leave it out. Clearly, $I_0 \subseteq K$.

Then, since m is an element of both $\bigcap_{i \notin K} A_i$ and $\bigcap_{i \notin I_0,\ i \in K} A_i$, it is clear that $m \in \bigcap_{i \notin I_0} A_i$.

From our definition of I_0, we know that $m \notin A_i$ for any $i \in I_0$. So, $m \in A_i^c$ for all $i \in I_0$. Then $m \in \bigcap_{i \in I_0} A_i^c$.

Therefore, $m \in \left[\bigcap_{i \in I_0} A_i^c \cap \bigcap_{i \notin I_0} A_i \right]$ and so, $m \in \bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right]$.

We have shown that:

$$\bigcap_{i \notin K} A_i \subseteq \bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right] . \tag{7}$$

From Equations 6 and 7, we may conclude that:

$$\bigcap_{i \notin K} A_i = \bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i \right] .$$

□

Lemma 5.2.

$$\sum_{I \subseteq K} |\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i| = |\bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i\right]| \ .$$

Proof. Note that it is sufficient to show that the sets in the union on the right-hand side are pairwise disjoint. We will show this by way of contradiction.

Suppose m is an element of both $\bigcap_{i \in H} A_i^c \cap \bigcap_{i \notin H} A_i$ and $\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i$ for H, $I \subseteq K$, $H \neq I$.

We now have several cases: $H \subset I$, $I \subset H$, or H and I are not subsets of one another. Without loss of generality, suppose $I \subset H$ or H and I are not subsets of one another. In either of these two cases, there exists l such that $l \in H$ but $l \notin I$.

Because $m \in A_i$ for all $i \notin I$, it is clear that $m \in A_l$. Similarly, because $m \in A_i^c$ for all $i \in H$, it is clear that $m \in A_l^c$. However, this contradicts the fact that m cannot be an element of both A_l and A_l^c. Therefore, what we assumed is false, and m cannot be an element of both $\bigcap_{i \in H} A_i^c \cap \bigcap_{i \notin H} A_i$ and $\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i$.

Thus, the sets in the union on the right side of the equation in Lemma 5.2 are pairwise disjoint, and so the size of their union is equal to the sum of their individual sizes.

□

We may now easily prove the following:

Theorem 5.1. *Let $A_1, A_2, \ldots, A_j$ be subsets of some set S, let $J = \{1, 2, \ldots, j\}$, and suppose K is a set of positive integers such that $K \subseteq J$. Then,*

$$|\bigcap_{i \notin K} A_i| = \sum_{I \subseteq K} |\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i| \ .$$

Proof. From Lemma 5.1, we know that

$$|\bigcap_{i \notin K} A_i| = |\bigcup_{I \subseteq K} \left[\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i\right]| \ .$$

Substituting in our result from Lemma 5.2, we see that

$$|\bigcap_{i \notin K} A_i| = \sum_{I \subseteq K} |\bigcap_{i \in I} A_i^c \cap \bigcap_{i \notin I} A_i| \ .$$

□

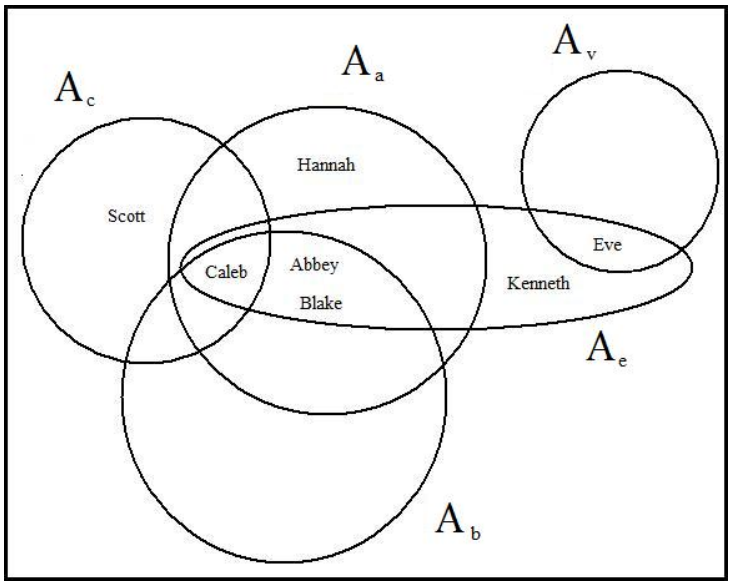

Figure 3: A Venn diagram illustrating the structure of the sets described in Example 5.1. The entire set S is the large box enclosing the A_δ's.

We mentioned at the beginning of this section that the proof of Theorem 5.1 is a bit galling. As a concrete illustration of the theorem's worth, consider the following example:

Example 5.1. Suppose we know 7 people, whose names are Caleb, Eve, Blake, Kenneth, Scott, Hannah, and Abbey. Our set S is the set of all 7 people, and the subset A_δ of S is the set of people who have at least one "δ" in their first name. Let $J = \{a, b, c, e, v\}$, and $K \subseteq J$ be equal to $\{a, b, c\}$. A visual description of this setup may be found in Figure 3. Theorem 5.1 tells us that:

$$|\bigcap_{\delta \notin K} A_\delta| = \sum_{I \subseteq K} |\bigcap_{\delta \in I} A_\delta^c \cap \bigcap_{\delta \notin I} A_\delta| \ .$$

The expression on the left tells us how many of these 7 people have both e's and v's in their first name. From simply counting, we see that the size of the set on the left is 1 (only Eve fits into this category). The expression on the right is a bit more cryptic. To understand what it is saying, we must evaluate

$$|\bigcap_{\delta \in I} A_\delta^c \cap \bigcap_{\delta \notin I} A_\delta|$$

for each subset I of K. In particular, we have $I = \emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, or $\{a, b, c\}$.

For $I = \emptyset$, we have $\bigcap_{\delta \in \emptyset} A_\delta^c$ representing the complement of the emptyset (which is the union of all of the A_δ's, and thus all 7 people), and $\bigcap_{\delta \notin \emptyset} A_\delta$ representing the intersection of all of the A_δ's, where $\delta \in \{a, b, c, e, v\}$ (that is, the emptyset). So, their intersection is the emptyset:

$$|\bigcap_{\delta\in\emptyset} A_\delta^c \cap \bigcap_{\delta\notin\emptyset} A_\delta| = |\{\text{Caleb, Eve, Blake, Kenneth, Scott, Hannah, Abbey}\} \cap \emptyset| = 0.$$

For $I = \{a\}$, we see that $\bigcap_{\delta\in\{a\}} A_\delta^c$ represents the complement of A_a (which includes exactly Scott, Kenneth, and Eve), and $\bigcap_{\delta\notin\{a\}} A_\delta$ represents the intersection of all of the A_δ's where $\delta \in \{b, c, e, v\}$ (that is, again, the emptyset). So, their intersection is the emptyset:

$$|\bigcap_{\delta\in\{a\}} A_\delta^c \cap \bigcap_{\delta\notin\{a\}} A_\delta| = |\{\text{Eve, Kenneth, Scott}\} \cap \emptyset| = 0.$$

We may evaluate this intersection for the other subsets of $\{a, b, c\}$ in a similar fashion, yielding the following.

For $I = \{b\}$,

$$|\bigcap_{\delta\in\{b\}} A_\delta^c \cap \bigcap_{\delta\notin\{b\}} A_\delta| = |\{\text{Eve, Kenneth, Scott, Hannah}\} \cap \emptyset| = 0.$$

For $I = \{c\}$,

$$|\bigcap_{\delta\in\{c\}} A_\delta^c \cap \bigcap_{\delta\notin\{c\}} A_\delta| = |\{\text{Eve, Blake, Kenneth, Hannah, Abbey}\} \cap \emptyset| = 0.$$

For $I = \{a, b\}$,

$$|\bigcap_{\delta\in\{a,b\}} A_\delta^c \cap \bigcap_{\delta\notin\{a,b\}} A_\delta| = |\{\text{Eve, Kenneth, Scott}\} \cap \emptyset| = 0.$$

For $I = \{a, c\}$,

$$|\bigcap_{\delta\in\{a,c\}} A_\delta^c \cap \bigcap_{\delta\notin\{a,c\}} A_\delta| = |\{\text{Eve, Kenneth}\} \cap \emptyset| = 0.$$

For $I = \{b, c\}$,

$$|\bigcap_{\delta\in\{b,c\}} A_\delta^c \cap \bigcap_{\delta\notin\{b,c\}} A_\delta| = |\{\text{Hannah, Eve, Kenneth}\} \cap \emptyset| = 0.$$

For $I = \{a, b, c\}$,

$$|\bigcap_{\delta\in\{a,b,c\}} A_\delta^c \cap \bigcap_{\delta\notin\{a,b,c\}} A_\delta| = |\{\text{Eve, Kenneth}\} \cap \{\text{Eve}\}| = 1.$$

Adding all of these up, we find that $\sum_{I\subseteq K} |\bigcap_{\delta\in I} A_\delta^c \cap \bigcap_{\delta\notin I} A_\delta| = 1$, as Theorem 5.1 foretold.

5.2 Proof Using Möbius Inversion

Theorems 4.1, 5.1 and 3.2 (that is, the Möbius inversion formula, our previous theorem, and the definition of the Möbius function on subsets of a set) allow us to prove the principle of inclusion and exclusion, which is stated below.

Theorem 5.2. *Let $A_1, A_2, \ldots, A_n \subseteq S$ where S is a finite set, and let $[n] = \{1, 2, 3, \ldots, n\}$. Then,*

$$|\bigcap_{i\in[n]} A_i^c| = \sum_{I\subseteq[n]} (-1)^{|I|} |\bigcap_{i\in I} A_i| \ .$$

Proof. Let $K \subseteq \{1, 2, 3, \ldots, n\} = [n]$. By Theorem 5.1, we know that:

$$|\bigcap_{i\notin K} A_i| = \sum_{I\subseteq K} |\bigcap_{i\in I} A_i^c \cap \bigcap_{i\notin I} A_i| \ .$$

Then, define $g(K) = |\bigcap_{i\notin K} A_i|$. By Theorems 4.1 and 3.2,

$$|\bigcap_{i\in K} A_i^c \cap \bigcap_{i\notin K} A_i| = \sum_{I\subseteq K} \mu(I, K) |\bigcap_{i\notin I} A_i| = \sum_{I\subseteq K} (-1)^{|K|-|I|} |\bigcap_{i\notin I} A_i| \ .$$

Letting $K = [n]$ and simplifying,

$$|\bigcap_{i\in[n]} A_i^c \cap \bigcap_{i\notin[n]} A_i| = |\bigcap_{i\in[n]} A_i^c| = \sum_{I\subseteq[n]} (-1)^{|[n]|-|I|} |\bigcap_{i\notin I} A_i| \ .$$

We find that the right-hand side of this equation is, in fact, the following sum, with the terms rearranged:

$$\sum_{I\subseteq[n]} (-1)^{|I|} |\bigcap_{i\in I} A_i| \ .$$

Then,

$$|\bigcap_{i\in[n]} A_i^c| = \sum_{I\subseteq[n]} (-1)^{|I|} |\bigcap_{i\in I} A_i| \ .$$

□

5.3 Derangements

As was mentioned at the beginning of this section, the principle of inclusion and exclusion is a tool for counting the number of objects that satisfy a given condition. Suppose we would like to count the number of *derangements* of a sequence. A derangement is defined as follows:

Definition 5.1. A *derangement* of the set $[n] = \{1, 2, 3, \ldots, n\}$ is a permutation $\pi : [n] \to [n]$ such that $\pi(i) \neq i$ for each $1 \leq i \leq n$.

For example, the only two derangements of $\{1, 2, 3\}$ are $\{3, 1, 2\}$ and $\{2, 3, 1\}$. The permutation $\{1, 3, 2\}$, for example, is not a derangement because 1 appears in its natural place (the first position). We will denote by D_n the set of all derangements of a set of n objects. Unsurprisingly, we find the size of D_n using the principle of inclusion and exclusion. Brualdi [1] offers the following theorem, and we will provide a proof.

Theorem 5.3. [1, p.168] *For $n \geq 1$,*

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\right) .$$

Proof. Let S be the set of all possible permutations of the set $\{1, 2, \ldots, n\}$, and let s_i, where $i \in \{1, 2, \ldots, n\}$, be the set of all permutations such that i falls in the ith position. Then,

$$|D_n| = |S \setminus (s_1 \cup s_2 \cup \ldots \cup s_n)| = |s_1^c \cap s_2^c \cap \ldots \cap s_n^c| .$$

From the principle of inclusion and exclusion (Theorem 5.2), we see that

$$|D_n| = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \Big|\bigcap_{i \in I} s_i\Big| . \tag{8}$$

This may seem a bit dense, but may be thought of in a very intuitive way.

Starting with the set S, we notice that to find D_n we must remove all permutations where any element of $\{1, 2, \ldots, n\}$ is in its "natural" position. In other words, we will subtract the sizes of all of the s_i's. Note that $|S| = n!$ and that if i is in its proper position, the other elements of the set have $(n-1)!$ ways of being arranged. So, $|S| - |s_1| - |s_2| - \ldots - |s_n| = n! - \binom{n}{1}(n-1)!$.

However, we have now subtracted some permutations several times. For instance, consider a permutation in which the 1st and the 5th elements are both in their "natural" positions. This permutation is in both the set s_1 and the set s_5, so we have subtracted it from S at least two times. To rectify this, we add the intersections of any two s_i's back in.

Our new sum is: $n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)!$. Following similar logic, however, and noticing that we continue to add and subtract "too much," we eventually arrive at the sum:

$$D_n = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \ldots + (-1)^{n-1}\binom{n}{n-1}(1)! + (-1)^n\binom{n}{n}(0)! \ .$$

The last term of this sum is simply the identity permutation, as we have chosen all n elements to be fixed in their "natural" positions. Note that this equality also comes directly from our application of the principle of inclusion and exclusion in Equation 8. Simplifying, we see that:

$$D_n = n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \ldots + (-1)^n\frac{n!}{n!0!}(0)! \ .$$

And so,

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n\frac{1}{n!}\right) \ .$$

□

Example 5.2. Ms.Nomer is a high school math teacher. Whenever she creates a new seating chart for her 5 honors students, she makes sure that no student remains in the desk assigned to them by the previous seating chart. If there are only 5 desks in the classroom, in how many different ways can she create a new seating chart?

In other words, we would like to find the number of derangements of $\{1, 2, 3, 4, 5\}$.

Viewed in the context of the principle of inclusion and exclusion and Theorem 5.3, this problem becomes relatively straightforward:

$$D_5 = 5!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!}\right) \ .$$

Simplifying,

$$D_5 = 5! - \frac{5!}{1!} + \frac{5!}{2!} - \frac{5!}{3!} + \frac{5!}{4!} - \frac{5!}{5!} = 120 - 120 + 60 - 20 + 5 - 1 = 44.$$

Therefore, there are 44 different ways to create a new seating chart for Ms.Nomer's 5 students so that no student remains in the same desk.

5.3.1 Probability

Brualdi [1] goes on to note that because $e^{-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!}$,

$$e^{-1} = \frac{D_n}{n!} + (-1)^{n+1}\frac{1}{(n+1)!} + (-1)^{n+2}\frac{1}{(n+2)!} + \dots$$

Recall that:

Theorem 5.4. [2, p.225] *If S is the sum of the convergent alternating series $\sum_{k=0}^{\infty}(-1)^k a_k$, and s_n is the nth partial sum of the series, then $|S - s_n| \leq a_{n+1}$ for each positive integer n.*

In the context of derangements, we see that $|e^{-1} - \frac{D_n}{n!}| \leq \frac{1}{(n+1)!}$. For the first few values of n, the right-hand side of the inequality is equal to $\frac{1}{2} = 0.5$, $\frac{1}{6} = 0.1\overline{6}$, $\frac{1}{24} = 0.041\overline{6}$, $\frac{1}{120} = 0.008\overline{3}$, $\frac{1}{720} = 0.00138\overline{8}$. Clearly, the error quickly becomes negligible.

Since $\frac{D_n}{n!}$ is exactly the probability of choosing a derangement from the set of all permutations of $\{1, 2, \dots, n\}$, we see that, for large enough n, this probability is essentially equal to $\frac{1}{e} \approx 0.3679$.

Example 5.3. A professor is handing homework assignments back to his 30 students. If he does not look at the names on the papers, but hands them back at random, what is the probability that no student will receive his or her own paper?

Essentially, we are asking what the probability is that we will create a derangement of a set of 30 objects. From our discussion above, we know that this probability is approximately equal to $\frac{1}{e}$. Thus, there is about a 37 percent chance that no student will receive his or her own paper.

6 Number Theory

In addition to having combinatorial applications, there is a number theoretic concept of Möbius inversion. Though its form is slightly altered, we will see that the version of the theorem found in number theory is parallel to our original statement of the Möbius inversion formula (see Theorem 4.1). Recall from Theorem 3.3 that, in the context of divisors of an integer, $\mu(a, b)$ depends only on the quotient $\frac{b}{a}$. So, we may understand the Möbius function evaluated at a single integer: $\mu(a, b) = \mu(\frac{b}{a})$. We will use this notation for the remainder of our discussion.

6.1 The Möbius Inversion Formula

We will make use of the following definition in our subsequent statement of the theorem:

Definition 6.1. A *number-theoretic function* is a function whose domain is the set of positive integers.

LeVeque [5] provides the following theorem. Note that it is merely a form of Theorem 4.1. We will include LeVeque's proof, but it may clearly be proven as a simple corollary of Theorem 4.1.

Theorem 6.1. [5, p.128] *If f is any number-theoretic function and*

$$F(n) = \sum_{d|n} f(d) \ ,$$

then

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}) = \sum_{d|n} F(\frac{n}{d})\mu(d) = \sum_{d_1 d_2 = n} \mu(d_1)F(d_2) \ .$$

Proof. Suppose that f is any number-theoretic function and

$$F(n) = \sum_{d|n} f(d) \ .$$

Then, if $d = d_1$ and $\frac{n}{d} = d_2$, $d_1 d_2 = n$ and

$$\sum_{d|n} F(\frac{n}{d})\mu(d) = \sum_{d_1 d_2 = n} \mu(d_1)F(d_2) \ .$$

From our definition of $F(n)$, we see that:

$$\sum_{d_1 d_2 = n} \mu(d_1)F(d_2) = \sum_{d_1 d_2 = n} \mu(d_1) \sum_{d|d_2} f(d) \ .$$

Since $d|d_2$ is equivalent to $d|\frac{n}{d_1}$, we see that the following is true:

$$\sum_{d_1 d_2 = n} \mu(d_1) \sum_{d|d_2} f(d) = \sum_{d_1 d|n} \mu(d_1)f(d) = \sum_{d|n} f(d) \sum_{d_1|\frac{n}{d}} \mu(d_1) \ .$$

The second and third properties of the Möbius function μ (see Definition 3.1) state that:

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

So,

$$\sum_{d|n} f(d) \sum_{d_1|\frac{n}{d}} \mu(d_1) = f(n)$$

since the only nonzero term of $\sum_{d_1|\frac{n}{d}} \mu(d_1)$ occurs when $d = n$. □

6.2 Results

Möbius inversion in the context of number theory leads to several interesting results. Before we examine one such result, we need the following definition:

Definition 6.2. The *Euler ϕ-function* evaluated at an integer m (written $\phi(m)$) is the number of positive integers $a \leq m$ which are relatively prime to m.

Recall that two integers are relatively prime if they have no common divisors. We will also make use of the following theorem:

Theorem 6.2. [5, p.56] *For $n > 0$,*

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

LeVeque [5] asserts the following:

Theorem 6.3.

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

Proof. Let $F(n) = n$ for $n \in \mathbb{Z}$. Then, from Theorem 6.2, we have:

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

Applying Theorem 6.1, it is clear that:

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

□

LeVeque [5] notes that the usual explicit formula for $\phi(n)$, $n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, may also be used to derive Theorem 6.3. However, Theorem 6.2 and the Möbius inversion formula give us a rather elegant alternative.

LeVeque [5] goes on to provide several exercises for his readers. We will walk through solutions to two such exercises as examples in order to further illustrate the relevance of the Möbius inversion formula.

Example 6.1. In this example, we will show that $\sum_{d^2|n} \mu(d) = |\mu(n)|$.

Let n be a positive integer. We have two cases: either n is divisible by some square greater than 1, or it is not.

In the first case, $|\mu(n)| = 0$, by Theorem 3.3.

We may write $n = n_1^2 n_2$, where n_2 is square-free (that is, no square greater than 1 divides n_2). Suppose d^2 divides n for some integer d. We may write d^2 uniquely as a product of primes, $d^2 = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where each of the m_i's is even. Then $p_i^{m_i}$ divides n for each $1 \leq i \leq k$.

Let $1 \leq i \leq k$, and suppose $p_i^{m_i}$ does not divide n_1^2. Then $p_i^{m_i - 1}$ must divide n_1^2, since n_2 is only divisible by, at most, p_i. So, the power on p_i in the prime decomposition of n_1^2 is odd. However, this contradicts the fact that n_1^2 is a square, and so must have even powers on all of its prime divisors. Thus, what we assumed is false, and $p_i^{m_i}$ divides n_1^2. So, $d^2 | n_1^2$. Clearly, the converse is also true: if $d^2 | n_1^2$, then $d^2 | n$. Then, we see that the following equality holds, where n_1 and n_2 are defined as above:

$$\sum_{d^2|n} \mu(d) = \sum_{d^2|n_1^2} \mu(d) \ .$$

Note that $d^2 | n_1^2$ if and only if $d | n_1$, and so:

$$\sum_{d^2|n_1^2} \mu(d) = \sum_{d|n_1} \mu(d) \ .$$

But, by the third property of the Möbius function, for $n_1 > 1$,

$$\sum_{d|n_1} \mu(d) = 0.$$

If $n_1 = 1$, then we have moved on to the instance in which n is square-free. There are no d^2's, where $d > 1$, that divide n, and so it is true that $|\mu(n)| = 1$, and

$$\sum_{d^2|n} \mu(d) = \mu(1) = 1.$$

In either case, we find that

$$\sum_{d^2|n} \mu(d) = |\mu(n)| \ .$$

Example 6.2. This example focuses on an application of the Möbius inversion formula to classical algebra. We will begin with several definitions to bring our reader up to speed.

Definition 6.3. A complex number $z = \cos(\alpha) + i\sin(\alpha) = e^{i\alpha}$ is called an *nth root of unity* if $z^n - 1 = 0$, and is a *primitive* nth root of unity if, in addition, $z^k - 1 \neq 0$ for $1 \leq k < n$.

Definition 6.4. The *nth cyclotomic polynomial,* $\Phi_n(x)$, is the monic polynomial of which the zeros are the distinct primitive nth roots of unity.

Let $n > 1$ and $\zeta_n = e^{2\pi i/n}$.

We note that ζ_n is a primitive nth root of unity. To see that this is true, note that $\left(e^{2\pi i/n}\right)^n - 1 = e^{2\pi i} - 1 = 1 - 1 = 0$, but that for $1 \leq k < n$, $\left(e^{2\pi i/n}\right)^k - 1 = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) - 1 = (\alpha - 1) + \beta i$, where $\alpha \neq 1$. So, $\zeta_n^k - 1 \neq 0$.

Consider, now, ζ_n^j, where $1 \leq j \leq n$ and j and n are relatively prime (denoted by $(j, n) = 1$). We claim that the ζ_n^js are exactly the distinct primitive nth roots of unity. We will begin by showing that a given ζ_n^j is an nth root of unity:

$$\left(\zeta_n^j\right)^n - 1 = \left(e^{2\pi ij/n}\right)^n - 1 = e^{2\pi ij} - 1 = \cos(2\pi j) + i\sin(2\pi j) - 1 = 1 - 1 = 0.$$

To see that ζ_n^j is a *primitive* nth root of unity, let $1 \leq k < n$, and consider:

$$\left(\zeta_n^j\right)^k - 1 = \left(e^{2\pi ij/n}\right)^k - 1 = e^{2\pi ijk/n} - 1 = \cos\left(\frac{2\pi jk}{n}\right) + i\sin\left(\frac{2\pi jk}{n}\right) - 1.$$

To show that the above sum is not equal to zero, we need only show that $\cos\left(\frac{2\pi jk}{n}\right) \neq 1$. To do so, it is sufficient to show that $\frac{jk}{n}$ is not an integer. By way of contradiction, suppose that this quotient is, indeed, an integer. Then, $n|jk$. Since n and j are relatively prime, it must be the case that $n|k$. However, this contradicts the fact that $k < n$. Thus, what we assumed is false, and $\frac{jk}{n}$ is not an integer. Then, ζ_n^j is a primitive nth root of unity.

Next, we must show that the ζ_n^j's are distinct. Suppose j and m are distinct integers between 1 and n, and that each is relatively prime to n. Then, $\zeta_n^j = e^{2\pi ij/n} = \cos\left(\frac{2\pi j}{n}\right) + i\sin\left(\frac{2\pi j}{n}\right)$ and $\zeta_n^m = e^{2\pi im/n} = \cos\left(\frac{2\pi m}{n}\right) + i\sin\left(\frac{2\pi m}{n}\right)$.

Looking only at the real parts of these two complex numbers, it is clear that $\cos\left(\frac{2\pi j}{n}\right) \neq \cos\left(\frac{2\pi m}{n}\right)$, since $\frac{2\pi j}{n}$ and $\frac{2\pi m}{n}$ lie in the same period of the sine function (namely, they are both in the interval $\left[\frac{2\pi}{n}, 2\pi\right]$). Then, $\zeta_n^j \neq \zeta_n^m$, and we have established uniqueness.

Lastly, to see that these are all of the primitive nth roots of unity, suppose $t > n$ or $(t, n) \neq 1$. In the first case, $\zeta_n^t = \zeta_n^n \zeta_n^{n-t} = \zeta_n^{n-t}$ (recall that ζ_n is an nth root of unity). Then, we may

restrict our attention to t's such that $(t,n) \neq 1$ but $1 \leq t \leq n$. Suppose $(t,n) = b > 1$. Then, $\left(\zeta_n^t\right)^{n/b} - 1 = e^{2\pi i t/b} - 1$. Since $\frac{t}{b}$ is an integer, $e^{2\pi i t/b} - 1 = 0$. But $\frac{n}{b} < n$ and so, by Definition 6.3, ζ_n^t is not a primitive root of unity.

We have shown that the ζ_n^j's are exactly the distinct primitive nth roots of unity. By Definition 6.4, we see that:

$$\Phi_n(x) = \prod_{1 \leq j \leq n,\ (j,n)=1} (x - \zeta_n^j) \ .$$

Next, we would like to show that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. We know, from the fundamental theorem of algebra, that $x^n - 1$ may be uniquely factored as a product of $(x - z_t)$'s, where the z_t's are the distinct nth roots of unity. So, if we can show that $\prod_{d|n} \Phi_d(x)$ is exactly this product, we are done.

We just showed that

$$\Phi_d(x) = \prod_{1 \leq j \leq d,\ (j,d)=1} (x - \zeta_d^j) \ ,$$

where $\zeta_d = e^{2\pi i/d}$. So,

$$\prod_{d|n} \Phi_d(x) = \prod_{d|n} \prod_{(1 \leq j \leq d,\ (j,d)=1)} (x - \zeta_d^j) \ . \tag{9}$$

We must show that the ζ_d^j's are exactly the n distinct nth roots of unity.

First, we will show that if $(x - \zeta_d^j)$ is a divisor of the product on the right in Equation 9, then ζ_d^j is an nth root of unity.

Suppose $(x - \zeta_d^j)$ is a divisor of the product in Equation 9. Then, $d|n$, and $\zeta_d^j = e^{2\pi i j/d}$ is a primitive dth root of unity, from our earlier findings. So, it is clear that $1 = \left(e^{2\pi i j/d}\right)^d = \left(e^{2\pi i j/d}\right)^{d(n/d)} = \left(e^{2\pi i j/d}\right)^n$, and so ζ_d^j is, by definition, an nth root of unity.

Next, we must show that all of the nth roots of unity show up in the product, and that each "$(x - z_t)$" occurs only once.

Consider z_t, an arbitrary nth root of unity. We have two cases: either z_t is a primitive nth root of unity, or it is not.

In the first case, since $n|n$, we know that the product $\prod_{1 \leq j \leq n,\ (j,n)=1} (x - \zeta_n^j)$ divides the right hand side of Equation 9, where the ζ_n^j's are exactly the primitive nth roots of unity (see our earlier discussion). So, $(x - z_t)$ clearly divides our product.

In the second case, there exists $1 \leq k < n$ such that $(z_t^k - 1) = 0$. Choose the minimum such k.

Then, z_t is a primitive kth root of unity. We claim that k divides n, and will prove our assertion by way of contradiction: suppose k does not divide n. Then, $1 = z_t^n = z_t^{mk} z_t^s = z_t^s$, where m is some positive integer and $1 \leq s < k$. However, this contradicts the fact that our chosen k is the smallest integer such that z_t is a kth root of unity. Then, what we assumed is false, and k must divide n. Then, $(x - z_t)$ is a divisor of the right-hand side of Equation 9 since $k|n$ and z_t is a primitive kth root of unity. From these two cases, we see that all nth roots of unity show up in Equation 9.

All that is left to show, then, is that "$(x - z_t)$" occurs only once for each distinct nth root z_t. As we saw earlier, each of the ζ_d^j's is distinct for a given d. So, suppose that we have $z_t = \zeta_{d_1}^{j_1} = \zeta_{d_2}^{j_2}$ for $d_1, d_2|n$, $d_1 \neq d_2$, $1 \leq j_1 \leq d_1$, $1 \leq j_2 \leq d_2$, $(j_1, d_1) = 1$ and $(j_2, d_2) = 1$.

Then, z is a primitive d_1st root of unity, and is also a primitive d_2nd root of unity. Without loss of generality, suppose $d_1 < d_2$. Then, $z^{d_1} - 1 = 0$, which contradicts the fact that z is a primitive d_2nd root of unity. Then, what we assumed is false and $d_1 = d_2$. For each distinct nth root of unity z_t, "$(x - z_t)$" occurs only once in the product of Equation 9. Thus, we have shown that $\prod_{d|n} \Phi_d(x)$ is exactly the product of the distinct $(x - z_t)$'s, where the z_t's are the n distinct nth roots of unity. Thus,

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \ . \tag{10}$$

We may apply the Möbius inversion formula (see Theorem 6.1) to Equation 10. Let $F(n) = \log(x^n - 1)$ and let $f(d) = \log(\Phi_d(x))$, and note that

$$\log(x^n - 1) = \log\left(\prod_{d|n} \Phi_d(x)\right) = \sum_{d|n} \log(\Phi_d(x))$$

implies, by the Möbius inversion formula, that

$$\log(\Phi_n(x)) = \sum_{d|n} \log(x^d - 1)\mu(\frac{n}{d}) = \sum_{d|n} \log(x^{n/d} - 1)\mu(d) \ .$$

Simplifying and rewriting using properties of logarithms,

$$\log(\Phi_n(x)) = \log \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} \ .$$

So,

$$(\Phi_n(x)) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} \ .$$

Note that the product on the right-hand side is the product of polynomials with integer coefficients. Thus, $\Phi_n(x)$ is a polynomial with integer coefficients. In other words, $\Phi_n(x) \in \mathbb{Z}[x]$.

7 Conclusion

We have moved from the basic concept of partially ordered sets up through compatible matrices and the Möbius function, arriving at long last at the principle of Möbius inversion and several resulting concepts in combinatorics, number theory, and classical algebra. Our discussion of compatible matrices was really only relevant in reference to the proofs of the existence and uniqueness of the Möbius function, and that of the Möbius inversion formula. While the Möbius function and the Möbius inversion formula are interesting in and of themselves, we have seen them used primarily as a stepping stones in proofs of other results. We see this, for example, in a nontraditional proof of the combinatorially significant principle of inclusion and exclusion.

Möbius inversion lies in the intersection of several branches of mathematics. Arguing for its inherent beauty is an irrelevant endeavor, as the reader's apparent interest in the subject has propelled them as far as this point, but do take a moment to ponder the satisfaction to be found in such a broadly applicable result. In more than a semester's work of thirty-six pages, this paper could go on to examine further implications of the Möbius inversion formula. Most unfortunately, we must, instead, halt our exploration at this point. However, the end of our narrative should not signal an end to the reader's curiosity: go forth and invert!

References

[1] R. A. Brualdi, *Introductory Combinatorics, 2nd ed.*, Prentice Hall, 1992.

[2] R. A. Gordon, *Real Analysis: A First Course, 2nd ed.*, Addison-Wesley, 2002.

[3] R. P. Grimaldi, *Discrete and Combinatorial Mathematics: an Applied Introduction, 3rd ed.*, Addison-Wesley, 1994.

[4] D. C. Lay, *Linear Algebra and its Applications, 3rd ed.*, Addison-Wesley, 2006.

[5] W. J. LeVeque, *Fundamentals of Number Theory*, Dover Publications, Inc., 1977.

[6] L. Lovász, *Combinatorial Problems and Exercises*, North-Holland Publishing Co., 1979.