

# Möbius Function of Partially Ordered Sets

## 1 Introduction

The theory of Möbius inversion gives us a unified way to look at many different results in combinatorics that involve inverting the relation between two functions, where one of the functions is expressed as a summation, over some index choice, of the other function. Thus this theory generalizes the principle of inclusion and exclusion. We consider the following four examples:

1. Finite Differences: Let  $f$  be a function on natural numbers. Define  $g(n) := \sum_{m \leq n} f(m)$ . How can we “invert” the relation, i.e., express  $f$  in terms of  $g$ ? In this case it is easy to see that  $f(m+1) = \Delta g = g(m+1) - g(m)$ .
2. Principle of Inclusion and Exclusion: Let  $S$  be a set of properties that elements of a universe set  $U$  satisfy. Given a set  $T \subseteq S$ , let  $f_=(T)$  be the number of elements in  $U$  with exactly the properties in  $T$ . Given this function it is easy to count the number of elements that have at least the properties in  $T$ , namely

$$f_{\geq}(T) = \sum_{Y \supseteq T} f_=(Y).$$

This is the easier part, expressing the “at least” in terms of the “exact”. How do we invert the relation? We had seen in the last lecture that the inverse is

$$f_=(T) = \sum_{Y \supseteq T} (-1)^{|Y \setminus T|} f_{\geq}(Y).$$

3. Classic Möbius Function: Let  $f$  be a function on natural numbers. Define

$$g(n) := \sum_{k|n} f(k).$$

How do we invert this relation? The answer was given by Möbius,

$$f(n) = \sum_{k|n} g(k) \mu(n/k)$$

where  $\mu(n)$  is the classical Möbius function

$$\mu(n) := \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ (-1)^{\text{number of distinct prime factors of } n} & \text{otherwise.} \end{cases}$$

4. Spanning sets of a Vector Space: How many subsets of the  $n$ -dimensional vector space  $V_n(q)$  over a finite field with  $q$  elements span the whole space, that is, how many distinct basis are there in the vector space  $V_n(q)$ ? Given a subspace  $U$ , let  $N_=(U)$  be the number of basis of  $V_n(q)$  that span  $U$ , and  $N_{\leq}(U)$  be the number of subsets of the vector space that span  $U$  or a subspace of  $U$ . Then it is clear that  $N_{\leq}(U) = \sum_{V \preceq U} N_=(V)$ , where  $V \preceq U$  means that  $V$  is a subspace of  $U$ . How do we invert this relation?

Note that in all the examples above, we want to invert a certain linear functional, i.e., solve for the summand function in terms of the new function. The summation is taken wrt certain “ordering”; in the first case it is  $\leq$ , in the second  $\subseteq$ , in the third it is divisibility; and in the fourth, it is  $\preceq$ , that is, “is a subspace of”. In the next section, we study a generalisation of all these orderings, and the goal is to invert a linear functional where the summation is done w.r.t. such a general ordering.

## 2 Partially Ordered Sets

A **partially ordered set**,  $P$ , poset for short, is a pair consisting of a set  $S$  and a relation  $\leq$  on  $S$  that is

- reflexive: for all  $x \in S$ ,  $x \leq x$ ;
- antisymmetric: for all  $x, y \in S$ , if  $x \leq y$  and  $y \leq x$  then  $x = y$ ;
- transitive: for all  $x, y, z \in S$ , if  $x \leq y$  and  $y \leq z$  then  $x \leq z$ .

As the name suggests, posets give us partial information on the ordering of the elements of  $S$  in absence of complete information. Note that in a poset two elements may be incomparable. A poset where this does not happen is called a **total order/linear order/chain**, i.e., for every pair  $x, y \in S$  either  $x \leq y$  or  $y \leq x$ . The sets and relation in all the four examples form a poset; in general, any collection of sets can be ordered to form a poset using the ordering by inclusion (which is the case for the fourth example). The **dual poset**  $P^*$  of  $P$  is obtained by reversing the ordering of elements in  $P$ .

An **induced sub-poset**  $Q$  of a poset  $P$  is a subset of  $P$  where the elements of  $Q$  carry over the ordering from  $P$ ; in particular, if  $P$  is a finite poset then there are  $2^{|P|}$  induced sub-posets of  $P$ . Of particular interest to us is a special sub-poset called an **interval**: for  $x, y \in P$ ,  $x \leq y$ , the (closed) interval  $[x, y]$  is the sub-poset consisting of all  $z \in P$  such that  $x \leq z \leq y$ ; thus a closed interval is never empty since the two endpoints always belong to it; open and half-open intervals can be defined similarly. If all intervals of  $P$  are finite, then  $P$  is called a **locally finite poset**. The set of integers is locally finite; the set of real numbers  $\mathbb{R}$  is not locally finite, since between any two real numbers there is an infinitude of real numbers; the poset of infinite subsets of an infinite set  $T$  is not locally finite. If  $x, y \in P$ , then we say  $y$  **covers**  $x$  if  $x < y$  and there is no  $z$  such that  $x \leq z \leq y$ , i.e.,  $x, y$  are the only two elements in the interval  $[x, y]$ . A locally finite set is completely described by its cover relations. For a finite poset, these relations can be picture as an undirected graph, called the **Hasse diagram**, over the elements of  $P$  such that there is an edge between  $x$  and  $y$  iff  $y$  covers  $x$ ; moreover, the vertex corresponding to  $y$  is placed “above” (with a higher vertical coordinate) than  $x$ .

Two posets  $P, Q$  are isomorphic,  $P \equiv Q$ , if there exists a bijective map  $\phi : P \rightarrow Q$  such that both  $\phi$  and  $\phi^{-1}$  are order preserving:

$$x \leq y \text{ in } P \iff \phi(x) \leq \phi(y) \text{ in } Q.$$

### 2.1 Generating new posets: Operations on posets

If  $P, Q$  be two posets on disjoint sets, then the **disjoint union or direct sum** of  $P$  and  $Q$  is the poset  $P + Q$  on the set  $P \cup Q$  such that  $x \leq y$  in  $P + Q$  if either (1)  $x, y \in P$  and  $x \leq y$  in  $P$ , or (2)  $x, y \in Q$  and  $x \leq y$  in  $Q$ . If the underlying sets of  $P, Q$  are not disjoint, then we label the underlying sets and take their union; more formally, we take the disjoint union of the underlying sets.<sup>1</sup> An **ordinal sum**  $P \oplus Q$  of two posets  $P, Q$  on disjoint sets is a poset that is a further restriction of  $P + Q$  in that  $x \leq y$  in  $P \oplus Q$ , if either it satisfies the two conditions of  $P + Q$ , or  $x \in P$  and  $y \in Q$ ; thus unlike the disjoint sum, an ordinal sum is not symmetric, i.e.,  $P \oplus Q \neq Q \oplus P$ . The **direct product**  $P \times Q$  of two posets  $P$  and  $Q$  is a poset on their cartesian product  $\{(x, y) : x \in P \text{ and } y \in Q\}$  such that  $(x, y) \leq (x', y')$  in  $P \times Q$  iff  $x \leq x'$  in  $P$  and  $y \leq y'$  in  $Q$ .

## 3 Möbius Function of Posets

Let  $P$  be a locally finite poset. Consider the set  $I(P)$  of all functions from the set  $\text{Int}(P)$  of closed intervals of  $P$  to  $\mathbb{R}$  (recall  $\emptyset \notin \text{Int}(P)$ ). For  $x, y \in P$  and  $f \in I(P)$ , if  $x \not\leq y$  then  $f(x, y) = 0$ , otherwise it is some value in  $\mathbb{R}$ . The set  $I(P)$  forms an  $\mathbb{R}$ -vector space, because addition of two functions and multiplication by scalar is defined as usual. We further define the product  $fg$  as a convolution:

$$fg(x, y) = \sum_{x \leq z \leq y} f(x, z)g(z, y). \quad (1)$$

<sup>1</sup>Given  $n$  sets  $A_1, \dots, A_n$  their disjoint union  $\sqcup_{i=1}^n A_i := \cup_{i=1}^n A_i^*$ , where  $A_i^* := \{(x, i) : x \in A_i\}$ .

With this additional property, it follows that  $I(P)$  forms an *associative algebra* over  $\mathbb{R}$ .<sup>2</sup> The set  $I(P)$  is called the **incidence algebra** of  $P$ . We now study some interesting functions in  $I(P)$ . Since it is a ring, a natural question to ask is what function is the multiplicative identity. It is not hard to see that it is the Kronecker delta:

$$\delta(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

Another interesting question is to characterise when does an  $f \in I(P)$  have an inverse. That is, when is there a  $g$  such that  $fg(x, y) = \delta(x, y)$ ? If  $x = y$ , then such a  $g$  must satisfy

$$f(x, x)g(x, x) = 1, \quad (3)$$

that is  $f(x, x) \neq 0$  for all  $x \in P$ , and if  $x < y$  then from (3) we obtain

$$g(x, y) = -f(x, x)^{-1} \sum_{x < z \leq y} f(x, z)g(z, y). \quad (4)$$

Thus given  $f$ , we can construct  $g$  in a top-down manner (that is, starting from the maximal elements, and considering intervals going down from them); e.g., if  $y$  covers  $x$  then

$$g(x, y) = -f(x, x)^{-1}f(x, y)g(y, y) = -f(x, x)^{-1}f(x, y)/f(y, y).$$

An interesting function in  $I(P)$  is the **zeta function**

$$\zeta(x, y) := \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

Thus  $\zeta(x, y)$  is an indicator function that tells us that  $x$  and  $y$  are comparable and  $x \leq y$ . This function plays a very important role. Let's see what does  $f\zeta$  mean:

$$f\zeta(x, y) = \sum_{x \leq z \leq y} f(x, z)\zeta(z, y) = \sum_{x \leq z \leq y} f(x, z).$$

Thus multiplying by  $\zeta$  is like “integrating” over the interval. Clearly,  $\zeta^2(x, y)$  is the cardinality of the interval  $[x, y]$ , i.e., the number of  $z$  such that  $x \leq z \leq y$ . Since by definition  $\zeta(x, x) = 1$ , from (5) and (6) it follows that  $\zeta$  has an inverse in  $I(P)$  called the Möbius function  $\mu$  of  $P$  and defined recursively as follows:

$$\mu(x, x) := 1 \text{ and } \mu(x, y) := - \sum_{x < z \leq y} \mu(z, y), \quad (6)$$

or even more succinctly as

$$\sum_{x \leq z \leq y} \mu(x, z) = \delta(x, y). \quad (7)$$

Given this definition, we can substitute  $g = \zeta$  and  $f = \mu$  in (6) to get

$$1 = - \sum_{x < z \leq y} \mu(x, z)$$

which is equivalent to

$$\mu(x, y) = - \sum_{x \leq z < y} \mu(x, z)$$

since  $\mu(x, x) = 1$ . What is the significance of  $\mu$ ? We have seen that multiplying by  $\zeta$  gives us a summation; multiplying by  $\zeta^{-1} = \mu$  inverts that relation. The following theorem makes this more precise:

---

<sup>2</sup>An associative  $R$ -algebra is an additive abelian group  $A$  which has the structure of *both a ring and an  $R$ -module* in such a way that ring multiplication is  $R$ -bilinear, i.e., commutes with the scalars:  $r \cdot (xy) = (r \cdot x)y = x(r \cdot y)$  for all  $r \in R$  and  $x, y \in A$ . Associative means that the multiplication operation  $A \times A \rightarrow A$  is associative. E.g., of non-associative multiplication is the cross-product in Euclidean space.

**Theorem 1 (Möbius Inversion Formula)** Let  $P$  be a locally finite poset and  $f : P \rightarrow \mathbb{R}$ . Moreover, assume that there exists an element  $\ell$  such that  $f(x) = 0$  when  $x \not\leq \ell$ , i.e., either  $x \leq \ell$  or is not comparable to  $\ell$ ; i.e., the function is zero outside the induced poset of elements that dominate  $\ell$ . If

$$g(x) := \sum_{y \leq x} f(y)$$

then

$$f(y) = \sum_{z \leq y} g(z) \mu(z, y).$$

The existence of  $\ell$  is needed so that the sum in the definition of  $g$  is well-defined; we can also say that in  $P$  every principal order ideal is finite. Also note that  $f, g \notin I(P)$ .

*Proof.* We want to verify that

$$f(y) = \sum_{z \leq y} g(z) \mu(z, y) = \sum_{z \leq y} \sum_{x \leq z} f(x) \mu(z, y) = \sum_{z \leq y} \sum_x f(x) \zeta(x, z) \mu(z, y)$$

By changing the order of summation, we obtain that the RHS is equal to

$$\sum_x f(x) \sum_{z \leq y} \zeta(x, z) \mu(z, y) = \sum_x f(x) \delta(x, y) = f(y)$$

as desired.

Another way to think about the inversion is as follows: the set of functions  $I(P)$  acts on a function  $f : P \rightarrow \mathbb{R}$  as a linear transformation: for  $\eta \in I(P)$  define

$$(f\eta)(x) := \sum_{y \leq x} f(y) \eta(y, x).$$

Then  $g = f\zeta$  and hence  $f = g\zeta^{-1} = g\mu$ .

**Q.E.D.**

**COROLLARY 2** Let  $P^*$  be the dual poset of  $P$ . Assume that there exists an element  $w$  such that  $f(x) = 0$  unless  $x \leq w$ . If

$$g(x) := \sum_{y \geq x} f(y)$$

then

$$f(y) = \sum_{z \geq y} g(z) \mu(y, z).$$

Another interesting function is the **incidence function**

$$\iota(x, y) := \zeta(x, y) - \delta(x, y), \tag{8}$$

which is zero when  $x = y$  or  $x$  and  $y$  are incomparable, and 1 when  $x < y$ . Multiplying the equation by  $\mu$ , we obtain

$$\iota\mu = \delta - \mu. \tag{9}$$

### 3.1 Constructing the Möbius Function Recursively

We had seen some ways to construct new posets from two posets. Can we construct the corresponding Möbius function in a similar manner? If two posets are isomorphic, then it is clear that their corresponding Möbius functions are the same, since  $\mu$  only depends upon the structure of the intervals.

Here we see the special case of direct product.

**Theorem 3 (Product Theorem)** Let  $P$  and  $Q$  be locally finite posets and  $P \times Q$  their direct product. If  $(x, y) \leq (x', y')$  then

$$\mu_{P \times Q}((x, y), (x', y')) = \mu_P(x, x') \mu_Q(y, y').$$

*Proof.* We want to show that

$$\delta((x, y), (x', y')) = \sum_{(x, y) \leq (u, v) \leq (x', y')} \mu_{P \times Q}((x, y), (u, v)).$$

Let us substitute the definition of  $\mu_{P \times Q}$  given above on the RHS to obtain

$$\begin{aligned} \sum_{(x, y) \leq (u, v) \leq (x', y')} \mu_{P \times Q}((x, y), (u, v)) &= \sum_{(x, y) \leq (u, v) \leq (x', y')} \mu_P(x, u) \mu_Q(y, v) \\ &= \sum_{x \leq u \leq x'} \mu_P(x, u) \sum_{y \leq v \leq y'} \mu_Q(y, v) \\ &= \delta(x, x') \delta(y, y'). \end{aligned}$$

But  $\delta(x, x') \delta(y, y')$  is one when  $x = x'$  and  $y = y'$ , that is, when  $(x, y) = (x', y')$ .

**Q.E.D.**

## 4 Applications

Let's see what is the Möbius function for our first example. Our poset is the set of positive integers ordered by absolute value. By definition  $\mu(n, n) = 1$ . Moreover, from (6) it follows that  $\mu(n-1, n) = -1$  and by induction  $\mu(k, n) = 0$  for  $k < n-1$ . Thus if  $g(n) := \sum_{m \leq n} f(m)$  then  $f(n) = \sum_{k \leq n} g(k) \mu(k, n) = g(n) - g(n-1)$ .

For the second example, we will use the product theorem Theorem 5 and the isomorphism property. Let  $\mathbf{2}$  be the poset formed by the numbers  $0, 1$ ; since  $\mathbf{2}$  is linearly ordered, its Möbius function is  $\mu(0, 0) = \mu(1, 1) = 1$  and  $\mu(0, 1) = -1$ ; succinctly,  $\mu(i, j) = (-1)^{i-j}$ . We can show that the poset over the power set of  $2^{[n]}$  is isomorphic to  $\mathbf{2}^n$ . Thus, any element in  $2^{[n]}$  can be represented by a boolean vector  $(x_1, \dots, x_n)$ ,  $x_i \in \{0, 1\}$ . Then for,  $T \subseteq S$ ,  $\mu(T, S) = \mu((t_1, \dots, t_n), (s_1, \dots, s_n))$ , which is equal to  $\prod_{i=1}^n \mu(t_i, s_i)$  by the product rule. But  $\mu(t_i, s_i) = (-1)^{s_i - t_i}$ . Thus

$$\mu(T, S) = \prod_{i=1}^n (-1)^{s_i - t_i} = (-1)^{\sum_i (s_i - t_i)} = (-1)^{|S| - |T|} = (-1)^{|S \setminus T|}.$$

The standard formula for PIE is obtained by applying Corollary 4 along with the Möbius function above.

Let  $\Delta_n$  be the poset over the set of divisors of  $n$ , where  $x \leq y$  if  $x$  divides  $y$ . Suppose  $n = p_1^{e_1} \dots p_t^{e_t}$  is the product of  $t$  primes. Then any divisor of  $n$  can be expressed as multiset  $\{p_1^{a_1}, \dots, p_t^{a_t}\}$ , and hence there is an isomorphism between the poset obtained by the direct product  $\mathbf{p}_1^{e_1} \times \mathbf{p}_2^{e_2} \dots \times \mathbf{p}_t^{e_t}$  and  $\Delta_n$ . The posets  $\mathbf{p}_i^{e_i}$  are linear orders, and hence the corresponding Möbius function is

$$\mu(p^i, p^j) = \begin{cases} 1 & \text{if } i = j \\ -1 & \text{if } i = j - 1 \\ 0 & \text{otherwise.} \end{cases}$$

Given two divisors  $a = \prod_i p_i^{a_i}$ ,  $b = \prod_i p_i^{b_i}$ ,  $a_i \leq b_i$  for all  $i$ , the Möbius function on the interval  $[a, b]$  is

$$\mu(a, b) = \mu\left(\prod_i p_i^{a_i}, \prod_i p_i^{b_i}\right) = \prod_i \mu(p_i^{a_i}, p_i^{b_i}) = \begin{cases} (-1)^{\sum_i (b_i - a_i)} & \text{if } b_i \in \{a_i, a_i + 1\} \\ 0 & \text{otherwise.} \end{cases}$$

From this it follows that  $\mu(a, b) = \mu(1, b/a)$  and this motivates the following classical definition of Möbius function which is another way to express the equation above: if  $a|b$  then

$$\mu(b/a) := \begin{cases} 1 & \text{if } a = b \\ (-1)^t & \text{if } b/a \text{ is a product of } t \text{ distinct primes} \\ 0 & \text{if } b/a \text{ is divisible by } p^2 \text{ for some prime } p. \end{cases} \quad (10)$$

Thus, if  $g(n) = \sum_{k|n} f(k)$  then

$$f(n) = \sum_{k|n} \mu(n/k)g(k),$$

which is the classic Möbius inversion formula from number theory. Before we show another application, we show how to derive a formula for Euler's totient function  $\phi(n)$ , which is the number of  $m \leq n$  that are relatively prime to  $n$ , using Möbius inversion. Define the set

$$S_d := \{m \leq n | \text{GCD}(m, n) = d\}. \quad (11)$$

Clearly two such sets are mutually disjoint; hence, the sets  $S_d$ 's, where  $d$  varies over all divisors of  $n$ , forms a partition of  $[n]$ . What is  $|S_d|$ ? Any  $m \in S_d$  is uniquely expressed as  $m = dk$ , where  $k$  is relatively prime to  $n/d$  (if not,  $d$  is not the gcd of  $m$  and  $n$ ); thus for a given choice of  $d$ , there are  $\phi(n/d)$  choices of  $k$ , which implies that  $|S_d| = \phi(n/d)$ . Combined with (13) we obtain that  $n = \sum_{d|n} \phi(n/d)$ . From the Möbius inversion formula it follows that

$$\phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d = \sum_{I \subseteq [n]} (-1)^{|I|} \frac{n}{p_I} = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

This formula can also be obtained by a direct application of PIE.

**¶1. Vector Spaces over Finite Fields** We now consider the fourth example given in the starting. Given an  $n$ -dimensional vector space  $V := V_n(q)$  over a field with  $q$  elements and  $U$  a subspace of  $V$ , How many distinct basis  $N_=(U)$  of  $U$  are there in  $V$ ? The problem reduces to computing the mobius function of the subspace lattice. But let's start with some easier questions. How many  $k$ -dimensional subspace of  $V$  are there? This number, denoted by  $\binom{n}{k}_q$ , surprisingly, acts quite analogous to the plain binomial coefficient. The binomial coefficient

$$\binom{n}{k} = \frac{\#\text{sequences of length } k \text{ from an } n\text{-element set}}{\#\text{sequences of length } k \text{ from an } k\text{-element set}} = \frac{n(n-1) \cdots (n-k+1)}{k!}.$$

Analogously, we have

$$\binom{n}{k}_q = \frac{\#\text{sequences of } k \text{ independent vectors from } V_n(q)}{\#\text{sequences of } k \text{ independent vectors from } V_k(q)}.$$

The numerator over-counts a  $k$ -dimensional subspace by the factor

$$\sum_{\text{basis of the } k\text{-dimensional space } V_k(q)} k!$$

which is exactly the quantity in the denominator. But what is the numerator? The first element can be chosen in  $(q^n - 1)$  ways, i.e., everything except the origin; for each such vector, all of its  $q$  scalings are linearly dependent, and include the origin, so the next linearly independent vector can be chosen in  $(q^n - q)$  ways; the two vectors chosen generate a subspace of size  $q^2$ , so the third vector can be chosen in  $(q^n - q^2)$  ways and so on. The same argument works for the denominator, and hence we have

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

The surprise is that

$$\lim_{q \rightarrow 1} \binom{n}{k}_q = \lim_{q \rightarrow 1} \frac{(1 + q + \cdots + q^{n-1}) \cdots (1 + q + \cdots + q^{n-k})}{(1 + q + \cdots + q^{k-1}) \cdots (1 + q)} = \binom{n}{k}.$$

To compute the Mobius function  $\mu(T, U)$ , for two subspaces  $T \preceq U \preceq V$ , we first show that the interval  $[T, U]$  is isomorphic to the interval  $[0, U/T]$  and hence the mobius function only depends on the dimension

of the two subspaces. This is not hard to see since the subspace structure in the interval is governed by a choice of an orthogonal basis  $v_1, \dots, v_{\dim(T)}, \dots, v_{\dim(U)}$  where the first  $\dim(T)$  elements span  $T$  and the rest span  $U$ ; the intermediate subspaces are obtained by adjoining different subsets of the last  $\dim(U) - \dim(T)$  elements. More formally, the map  $\pi$  that sends the first  $\dim(T)$  elements of a basis of  $U$  to zero and fixes the remaining elements gives us an isomorphism between  $[T, U]$  and  $[0, U/T]$ , where  $0$  denotes the subspace with one element, namely the origin.

Let  $\mu_n := \mu(0, V_n(q))$ . The proof idea is to count the number of 1-1 linear transformations from  $V_n(q)$  to another vector space  $X$ , over the same base field, with  $x \geq q^n$  vectors in two ways. For every subspace  $U$ , let  $M_=(T)$  be the number of linear maps  $f : V_n \rightarrow X$  such that  $T$  is the kernel of  $f$ , and  $M_\geq(T)$  be the number of linear maps  $f : V_n \rightarrow X$  such that  $T$  is contained in the kernel of  $f$ . Clearly,

$$M_\geq(T) = \sum_{T \preceq U} M_=(U)$$

and hence by Mobius inversion

$$M_=(T) = \sum_{T \preceq U} \mu(T, U) M_\geq(U).$$

In particular, for  $T = 0$  we have

$$M_=(0) = \sum_{0 \preceq U} \mu(0, U) M_\geq(U). \quad (12)$$

By definition,  $M_=(0)$  is the number of 1-1 linear maps from  $V_n$  to  $X$ . Each such map is specified uniquely by a *bijective* mapping of an *ordered sequence* of  $n$  linearly independent vectors to  $X$ ; changing the ordering gives us a different linear map (think of permutations). Similar to what was argued earlier, we obtain that

$$M_=(0) = (x - 1)(x - q) \cdots (x - q^{n-1}).$$

The quantity  $M_\geq(U)$  is the number of linear maps that map  $U$  to zero. If  $v_1, \dots, v_n$  is a basis for  $V_n$  where  $v_1, \dots, v_{\dim(U)}$  is a basis for  $U$  then such a linear map will map the first  $\dim(U)$  vectors to zero and the remaining  $n - \dim(U)$  vectors to any vector in  $X$  (possibly zero, since the kernel only needs to include  $U$ ); here we are using the fact that a linear map is completely determined by its action on a basis for the vector space. Therefore,  $M_\geq(U) = x^{n - \dim(U)}$ . Substituting these in the Mobius inversion formula (14) and equating the constant term we get

$$\mu(0, V_n) = (-1)^n q^{\binom{n}{2}}.$$

As  $q \rightarrow 1$  this is the same as the mobius function in the boolean algebra case.