

On a connection between max-min identity and GCD-LCM one over partially ordered set

Hongyan YU^{①*}

① College of mathematics and statistics, Hubei Normal University, Huangshi, Hubei, China 435002
E-mail: yhy710502@163.com

Received: 06-10-2011; Accepted: 07-25-2011 *Corresponding author

This research is supported by the Natural Science Foundation of Hubei Province, China (2007ABA124) and the Foundation of Hubei Normal University for Youth (2008D35).

Abstract In this paper we discuss two partially ordered sets and give a connection between max-min identity and GCD-LCM one.

Key Words partially ordered set, max-min identity, GCD-LCM identity, Inclusion-Exclusion principle

MSC 2010 06A07 11A05

1 Introduction

We know the fundamental theorem of arithmetic is an important result in number theory. The fact that every positive integer has a unique factorization into primes is special property in the set of integers. we discuss a connection between max-min functions and GCD-LCM by the fundamental theorem of arithmetic. The fundamental theorem of arithmetic asserts that every positive integer n greater than 1 can be written uniquely as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k},$$

where p_i is prime, $p_1 < p_2 < p_3 < \dots < p_k$ and $\alpha_i \geq 0, i = 1, 2, \dots, k$. Called the standard form of the prime-factorization of n . If this factorization is given, we can immediately deduce whether a prime p divides n since p divides n if and only if it is appears in this factorization. Denote $\max(a_1, a_2, \dots, a_k)$ ($\min(a_1, a_2, \dots, a_k)$) the maximal (minimal) real number of the set $\{a_1, a_2, \dots, a_k\}$. Note that GCD (Greatest Common Divisor) and LCM (Least Common Multiple) functions are

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} p_3^{\max(\alpha_3, \beta_3)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

and

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} p_3^{\min(\alpha_3, \beta_3)} \dots p_k^{\min(\alpha_k, \beta_k)}.$$

Also, we denote $(a_1, a_2, a_3, \dots, a_k) = (a_1, (a_2, \dots, a_k))$ and $[a_1, a_2, a_3, \dots, a_k] = [a_1, [a_2, \dots, a_k]]$ for $k > 2$.

In this paper we discuss two partially ordered sets and give a connection between max-min identity and GCD-LCM identity over partially ordered set. We discuss the Equivalence and uniformity of inclusion-exclusion principle in combinatorics, the total probability formula in probability theory, max-min identity and GCD-LCM one in number theory. Then some examples are given.

2 Max-Min functions and Partially ordered set

In this section, we first state some results of Max and Min functions needed later in the paper.

Lemma 2.1([1]). *If x and y are real numbers, then*

$$\max(x, y) + \min(x, y) = x + y.$$

Proof. If $x \geq y$, then $\min(x, y) = y$ and $\max(x, y) = x$, so that $\max(x, y) + \min(x, y) = x + y$. If $x < y$, then $\min(x, y) = x$ and $\max(x, y) = y$, we find again that $\max(x, y) + \min(x, y) = x + y$. \square

Lemma 2.2. *If x_1, x_2, \dots, x_k are real numbers, then $\max(x_1, x_2, \dots, x_k) = \max(x_1, \max(x_2, \dots, x_k))$.*

Lemma 2.3. *If x_1, x_2, \dots, x_k are real numbers, then $\min(x_1, x_2, \dots, x_k) = \min(x_1, \min(x_2, \dots, x_k))$.*

A partially ordered set (poset) \mathbf{P} is set, together with a binary relation denoted \leq_P , satisfying the following three axioms:

- (1) For all $x \in \mathbf{P}$, $x \leq_P x$; (reflexivity)
- (2) If $x \leq_P y$ and $y \leq_P x$, then $x = y$; (antisymmetry)
- (3) If $x \leq_P y$ and $y \leq_P z$, then $x \leq_P z$. (transitivity).

Definition 2.4([1]). *Two poset \mathbf{P} and \mathbf{Q} are isomorphic if exists an order-preserving bijection $\varphi : \mathbf{P} \rightarrow \mathbf{Q}$ whose inverse is order-preserving, that is, $x \leq y$ in $\mathbf{P} \Leftrightarrow \varphi(x) \leq \varphi(y)$ in \mathbf{Q} .*

Definition 2.5. *A chain (linear ordered set) is a poset in which any two elements are comparable.*

Sets are partially ordered by containment. More generally, in a lattice L , we can define a partial order \leq_L compatible with the lattice operations on L by $x \leq_L y$ if and only if $x \wedge y = x$. It is easy to prove that $x \wedge y = x$ if and only if $x \vee y = y$. Thus the following three conditions are equivalent:

$$x \leq_L y \Leftrightarrow x \wedge y = x \Leftrightarrow x \vee y = y.$$

Example 2.6. *Let A and B are nonempty sets. Then $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.*

Example 2.7. *Let x and y are positive integers. Then $x \leq y \Leftrightarrow \min(x, y) = x \Leftrightarrow \max(x, y) = y$.*

Example 2.8. *Let a and b are positive integers. Then $a \mid b \Leftrightarrow (a, b) = a \Leftrightarrow [a, b] = b$.*

Lemma 2.9([1]). *If a and b are positive integers, then $a, b = ab$.*

3 Main results

Theorem 3.1. *Let $x_1, x_2, x_3, \dots, x_n$ are positive integers and $n_1 = x_1, n_2 = \max(x_1, x_2), n_3 = \max(x_1, x_2, x_3), \dots, n_k = \max(x_1, x_2, x_3, \dots, x_k)$, then $[n] = \{n_1, n_2, \dots, n_k\}$ is a chain.*

Proof. Since $x_1 \leq \max(x_1, x_2) \leq \max(x_1, x_2, x_3) \leq \dots \leq \max(x_1, x_2, x_3, \dots, x_k)$, then $n_1 \leq n_2 \leq \dots \leq n_k$, that is $[n] = \{n_1, n_2, \dots, n_k\}$ is chain. \square

Theorem 3.2. *Let $m_1 = x_1, m_2 = \min(x_1, x_2), m_3 = \min(x_1, x_2, x_3), \dots, m_k = \min(x_1, \dots, x_k)$, then $[m] = \{m_1, m_2, \dots, m_k\}$ is a chain.*

Proof. Since $x_1 \geq \min(x_1, x_2) \geq \min(x_1, x_2, x_3) \geq \dots \geq \min(x_1, x_2, x_3, \dots, x_k)$, then $m_1 \geq m_2 \geq \dots \geq m_k$, that is $[m] = \{m_1, m_2, \dots, m_k\}$ is a chain. \square

Theorem 3.3. *Let $p_1 = a_1, p_2 = [a_1, a_2], p_3 = [a_1, a_2, a_3], \dots, p_k = [a_1, a_2, a_3, \dots, a_k]$, then $[p] = \{p_1, p_2, \dots, p_k\}$ is a chain.*

Proof. Since $a_1 \leq_{[p]} [a_1, a_2] \leq_{[p]} [a_1, a_2, a_3] \leq_{[p]} \dots \leq_{[p]} [a_1, a_2, a_3, \dots, a_k]$, then $p_1 \leq_{[p]} p_2 \leq_{[p]} \dots \leq_{[p]} p_k$ where $\leq_{[p]}$ is $|$, that is $[p] = \{p_1, p_2, \dots, p_k\}$ is a chain. \square

Theorem 3.4. *Let $q_1 = b_1, q_2 = (b_1, b_2), q_3 = (b_1, b_2, b_3), \dots, q_k = (b_1, b_2, b_3, \dots, b_k)$, then $[q] = \{q_1, q_2, \dots, q_k\}$ is a chain.*

Proof. Since $b_1 \geq_{[q]} (b_1, b_2) \geq_{[q]} (b_1, b_2, b_3) \geq_{[q]} \dots \geq_{[q]} (b_1, b_2, b_3, \dots, b_k)$, then $q_1 \geq_{[q]} q_2 \geq_{[q]} \dots \geq_{[q]} q_k$ where $\geq_{[q]}$ is $|$, that is $[q] = \{q_1, q_2, \dots, q_k\}$ is a chain. \square

Theorem 3.5. *Let $[n] = \{n_1, n_2, \dots, n_k\}$ and $[p] = \{p_1, p_2, \dots, p_k\}$, then there is an isomorphic between $[n]$ and $[p]$, where order preserving bijection $\varphi : [n] \rightarrow [p]$, that is $\varphi : n_i \leq n_{i'} \rightarrow p_i | p_{i'}$.*

Proof. Since $\varphi : n_i \leq n_{i'} \rightarrow p_i | p_{i'}$ and $n_i \leq n_{i'} \Leftrightarrow \max(n_i, n_{i'}) = n_{i'}$, $p_i | p_{i'} \Leftrightarrow [p_i, p_{i'}] = p_{i'}$. Thus, there is an isomorphic between $[n]$ and $[p]$. \square

Theorem 3.6. *Let $[m] = \{m_1, m_2, \dots, m_k\}$ and $[q] = \{q_1, q_2, \dots, q_k\}$, then there is an isomorphic between $[m]$ and $[q]$, where order preserving bijection $\varphi : [m] \rightarrow [q]$, that is $\varphi : m_j \leq m_{j'} \rightarrow q_j | q_{j'}$.*

Proof. Since $\varphi : m_j \leq m_{j'} \rightarrow q_j \leq q_{j'}$ and $m_j \leq m_{j'} \Leftrightarrow \min(m_j, m_{j'}) = m_j$, $q_j | q_{j'} \Leftrightarrow (q_j, q_{j'}) = q_j$. Thus, there is an isomorphic between $[m]$ and $[q]$. \square

Every chain is a lattice. Let $X = \{x_1, x_2, x_3, \dots, x_n\}$ is positive integers set, here we have $x \wedge y = \min(x, y)$ and $x \vee y = \max(x, y)$. Then (X, \max, \min, \leq) is a lattice. Let $A = \{a_1, a_2, a_3, \dots, a_n\}$ is positive integers set and we have $a \wedge b = (a, b)$ and $a \vee b = [a, b]$, then $(A, (,), [,], |)$ is a lattice. Let $P(A) = \{A_1, A_2, A_3, \dots, A_n\}$ is power set of set A , we also have $A \wedge B = A \cap B$ and $A \vee B = A \cup B$, then $(P(A), \cap, \cup, \subseteq)$ is a lattice.

Definition 3.7([4]). *If L and M are \vee -semilattices then $f : L \rightarrow M$ is said to be a \vee -morphism if $f(x \vee y) = f(x) \vee f(y)$ for all $x, y \in L$.*

Theorem 3.8([4]). *Lattices L, M are isomorphic if and only if there is a bijection $f : L \rightarrow M$ that is a \vee -morphism.*

Theorem 3.9. *Let X and Y are integer sets and $|X| = |Y|$, then $(X, \max, \min, \leq) \simeq (Y, (,), [,], |)$.*

Next we give two examples.

Example 3.10([1]). *If x, y, z are positive integers, then $\max(x, y, z) = x + y + z - \min(x, y) - \min(x, z) - \min(y, z) + \min(x, y, z)$.*

Proof. Without loss of generality, suppose that $x \leq y \leq z$, then $\max(x, y, z) = z, \min(x, y) = x, \min(y, z) = y, \min(x, z) = x, \min(x, y, z) = x$. Hence $x + y + z - \min(x, y) - \min(x, z) - \min(y, z) + \min(x, y, z) = x + y + z - x - y - x + x = z = \max(x, y, z)$. \square

Example 3.11. *If a, b, c are positive integers, then*

$$[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}.$$

Proof. By Theorem 3.8 and Example 3.11, $\max(x, y, z) \mapsto [a, b, c], x + y + z \mapsto abc, -\min(x, y) - \min(x, z) - \min(y, z) \mapsto (a, b)^{-1}(a, c)^{-1}(b, c)^{-1}, \min(x, y, z) \mapsto (a, b, c)$. then $[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}$. \square

In the following we give a max-min identity. The max-min identity is a relation between the maximum element of a set S of n numbers and the minima of the $2^n - 1$ nonempty subsets of S .

Theorem 3.12([5]). Let $S = \{x_1, x_2, x_3, \dots, x_n\}$ is a real number set, then $\max(x_1, x_2, x_3, \dots, x_n) = \sum_{i=1}^n x_i - \sum_{i<j} \min(x_i, x_j) + \sum_{i<j<k} \min(x_i, x_j, x_k) - \dots (-1)^{n+1} \min(x_1, x_2, x_3, \dots, x_n)$.

Conversely, we have

Theorem 3.13. Let $S = \{x_1, x_2, x_3, \dots, x_n\}$ is a real number set, then $\min(x_1, x_2, x_3, \dots, x_n) = \sum_{i=1}^n x_i - \sum_{i<j} \max(x_i, x_j) + \sum_{i<j<k} \max(x_i, x_j, x_k) - \dots + (-1)^{n+1} \max(x_1, x_2, x_3, \dots, x_n)$.

Corollary 3.14([5]). For any n Random Variables X_1, X_2, \dots, X_n , then $E[\max(x_1, \dots, x_n)] = \sum_{i=1}^n E[x_i] - \sum_{i<j} E[\min(x_i, x_j)] + \sum_{i<j<k} E[\min(x_i, x_j, x_k)] - \dots (-1)^{n+1} E[\min(x_1, x_2, \dots, x_n)]$.

Theorem 3.15. Let $a_1, a_2, a_3, \dots, a_n$ are positive integers, then

$$[a_1, a_2, a_3, \dots, a_n] = a_1 a_2 a_3 \dots a_n (a_1, a_2)^{-1} \dots (a_{n-1}, a_n)^{-1} (a_1, a_2, a_3) \dots (a_1, a_2, \dots, a_n)^{(-1)^{n+1}}.$$

Corollary 3.15. If $a_1, a_2, a_3, \dots, a_n$ are pairwise relatively primes integers, then $[a_1, a_2, a_3, \dots, a_n] = a_1 a_2 a_3 \dots a_n$.

Theorem 3.16. Let $a_1, a_2, a_3, \dots, a_n$ are positive integers, then

$$(a_1, a_2, a_3, \dots, a_n) = a_1 a_2 a_3 \dots a_n [a_1, a_2]^{-1} \dots [a_{n-1}, a_n]^{-1} [a_1, a_2, a_3] \dots [a_1, a_2, \dots, a_n]^{(-1)^{n+1}}.$$

4 Further topics and examples

In the theory of combinatorics, the inclusion-exclusion principle(also known as the sieve principle) is an equation related the size of two sets and their intersection. It states that if A and B are finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

For the general case of principle, in [6], let $\{A_1, A_2, \dots, A_n\}$ be finite sets. Then

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|,$$

where $|A|$ denotes the cardinality of the set A .

Example 4.1(Prime approximately formula). Let N is a positive integer, p_1, p_2, \dots, p_m are all prime integers less than \sqrt{N} , then

$$\pi(N) = m - 1 + N - \sum_{1 \leq i_1 \leq m} \left[\frac{N}{p_{i_1}} \right] + \sum_{1 \leq i_1 \leq i_2 \leq m} \left[\frac{N}{p_{i_1} p_{i_2}} \right] - \dots + (-1)^m \left[\frac{N}{p_{i_1} \dots p_m} \right].$$

Example 4.2 (Euler function formula). Let N is a positive integer, $\varphi(n)$ denotes numbers of relatively prime with n in $1, 2, \dots, N$, then

$$\varphi(n) = N \prod_{p|N} \left(1 - \frac{1}{p}\right).$$

In the theory of probability (see [5]), for events A_1, A_2, \dots, A_n in a probability space $(\Omega, \mathbf{F}, \mathbf{P})$, the inclusion-exclusion principle becomes in general the following form:

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i) - \sum_{1 \leq i < j \leq n} P(A_i \cap A_j) + \sum_{1 \leq i < j < k \leq n} P(A_i \cap A_j \cap A_k) - \dots + (-1)^{n-1} P(A_1 \cap A_2 \cap \dots \cap A_n),$$

where $P(A_i)$ denotes the probability of the event A_i .

Example 4.3 (The derangement problem). How many permutation $\pi \in \mathfrak{S}_n$ have no fixed points? Such a permutation is called a derangement. call this number $D(n)$, then

$$D(n) = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!}\right)$$

and indeed it is to show that $D(n)$ is nearest integer to $\frac{n!}{e}$. Thus the probability of an order for a shuffled deck of cards and being incorrect about every card is approximately $\frac{1}{e}$ ($\approx 37\%$). Thus formally the Principle of Inclusion-Exclusion is equivalent to the identity $(e^x)^{-1} = e^{-x}$.

In [2], Equivalence and uniformity of inclusion-exclusion principle in combinatorics, the total probability formula in probability theory are given. Let S be an n -set. Let V be the 2^n -dimensional vector space (over some field k) of all functions $f : 2^S \rightarrow k$. Let $\phi : V \rightarrow V$ be a linear transformation defined by

$$\phi f(T) = \sum_{Y \supseteq T} f(Y),$$

for all $T \subseteq S$, then ϕ^{-1} exists and is given by

$$\phi^{-1} f(T) = \sum_{Y \supseteq T} (-1)^{|Y-T|} f(Y),$$

for all $T \subseteq S$.

We discuss equivalence and correspondence between max-min identity and GCD-LCM identity in this paper. Our goal is to give a connection between max-min function and GCD-LCM over partially ordered set. As we known, complexity degree of algorithm between to prove max-min identity and GCD-LCM identity are very different in computation number theory.

References

- 1 Kenneth H. Rosen., Elementary number theory and its applications(Fourth Edition), China Machine Press, 2004.
- 2 Richard P. Stanley, Enumerative combinatorics (Vol 1), China Machine Press, 2004.
- 3 Joseph P.S. Kung, Gian-Carlo Rota, Catherine H. Yan., Combinatorics: The Rota Way, Cambridge University Press, 2009.
- 4 Blyth T.S., Lattices and ordered algebraic structures, Springer-Verlag, 2005.
- 5 Sheldon Ross, A first course in probability(sixth edition), Prentice Hall Inc., 2002.
- 6 Miklós Bóna, Introduction to enumerative combinatorics, The McGraw-Hill Companies Inc., 2007.