Proof Book

Updated Oct 17 2018

Relation and Partitions

Lemma 1.1: $\pi_1 \leq \pi_2$ **if and only if** $B_{\pi_1}(r) \subseteq B_{\pi_2}(r)$ **for all** r

Proof:

($\Rightarrow$) By definition, if $\pi_1 \leq \pi_2$, then for any r, there exists a block $B_{\pi_2}(t)$ such that $B_{\pi_1}(r) \subseteq B_{\pi_2}(t)$. It follows that $r \in B_{\pi_2}(t)$. Since $B_{\pi_2}(t) = B_{\pi_2}(r)$, we have $B_{\pi_1}(r) \subseteq B_{\pi_2}(r)$.

($\Leftarrow$) The definition of $\pi_1 \leq \pi_2$ follows immediately. $\square$

Theorem 1.1: $\pi_1 \leq \pi_2$ **if and only if** $s \equiv t(\pi_1) \Rightarrow s \equiv t(\pi_2)$

Proof:

($\Rightarrow$) Since $\pi_1 \leq \pi_2$, $B_{\pi_1}(r) \subseteq B_{\pi_2}(r)$ for all r from definition. Now suppose $s \equiv t(\pi_1)$ and $s \neq t(\pi_2)$. Since $ s\equiv t(\pi_1)$, $t \in B_{\pi_1}(s)$. Plus $B_{\pi_1}(s) \subseteq B_{\pi_2}(s)$, we have $t \in B_{\pi_2}(s)$, which means $s \equiv t(\pi_2)$, a contradiction to $s \neq t(\pi_2)$.

($\Leftarrow$) Assume it is not the case that $B_{\pi_1}(r) \subseteq B_{\pi_2}(r)$. Then for some u, $u \in B_{\pi_1}(r)$ but $u \notin B_{\pi_2}(r)$. Because $u \in B_{\pi_1}(r)$, $u \equiv r(\pi_1)$. Since $s \equiv t(\pi_1) \Rightarrow s \equiv t(\pi_2)$, we have $u \equiv r(\pi_2)$, and $u \in B_{\pi_2}(r)$, which produces a contradiction. $\square$

Corollary 1.1: $\leq: \pi_1 \rightarrow \pi_2$ **is a surjective function**

$\leq$ as a function is obvious from theorem 1.1.

$\leq$ must be surjective because suppose there is a $B_{\pi_2}(t)$ such that it contains no block in π_1. Yet for $B_{\pi_1}(t)$, there must be a block in π_2 such that $B_{\pi_1}(t) \subseteq B_{\pi_2}(t)$, which is a contradiction.

Partition Algebra

Lemma 2.1: $s \neq t(\pi_1) \vee s \neq t(\pi_2) \Rightarrow s \neq t(\pi_1 \cdot \pi_2)$

Proof: Assume $s \neq t(\pi_1) \wedge s = t(\pi_1 \cdot \pi_2)$.

Because $s = t(\pi_1 \cdot \pi_2)$, $s = t(\pi_1) \wedge s = t(\pi_2)$ followed from definition.

This contradicts $s \neq t(\pi_1)$. Proof is similar for π_2. $\square$

Lemma 2.2: $B_{\pi_1 \cdot \pi_2}(s) \subseteq B_{\pi_1}(s), B_{\pi_2}(s)$

Proof: It follows immediately from the definition that $B_{\pi_1 \cdot \pi_2}(s) = B_{\pi_1}(s) \cap B_{\pi_2}(s)$.$\square$

Theorem 2.1: $|\pi_1 \cdot \pi_2| \geq |\pi_1|, |\pi_2|$

Proof: Because $B_{\pi_1 \cdot \pi_2}(s) \subseteq B_{\pi_1}(s)$ for any $s \in S$ [lemma 2.2], for any block in π_1, there is a corresponding block in $\pi_1 \cdot \pi_2$ bounded by it (this correspondence is injective [lemma 2.1]). Hence, for all k blocks B in π_1, there are k blocks B' in $\pi_1 \cdot \pi_2$ such that $|B_1'| + |B_2'| + ...|B_k'| \leq |B_1| + |B_2| + ... + |B_k| = |S|$. It follows immediately that the number of blocks in $\pi_1 \cdot \pi_2$ is at least k. Proof is similar for π_2. $\square$

Theorem 2.2: $\pi_1 \leq \pi_2 \Rightarrow \pi_1 \cdot \pi_2 = \pi_1$

Proof: Because $\pi_1 \leq \pi_2$, we have $s \equiv t(\pi_1) \Rightarrow s \equiv t(\pi_2)$ for all $s, t \in S$. It follows that $s \equiv t(\pi_1) \Rightarrow s \equiv t(\pi_1 \cdot \pi_2)$. This means $B_{\pi_1}(s) \subseteq B_{\pi_1 \cdot \pi_2}(s)$ for all s [theorem 1.1]. Since it's always true that $B_{\pi_1 \cdot \pi_2}(s) \subseteq B_{\pi_1}(s)$ for all s [lemma 2], we have $B_{\pi_1 \cdot \pi_2}(s) = B_{\pi_1}(s)$ for all s. Therefore, $\pi_1 \cdot \pi_2 = \pi_1$. $\square$

Theorem 2.3: Partition multiplication is associative.

Proof: We need to show that $\pi_1 \cdot \pi_2 = \pi_2 \cdot \pi_1$. The set $\pi_1 \cdot \pi_2$ is $\{B \mid s, t \in B, s \equiv t(\pi_1) \wedge s \equiv t(\pi_2)\}$. The set $\pi_2 \cdot \pi_1$ is $\{B \mid s, t \in B, s \equiv t(\pi_2) \wedge s \equiv t(\pi_1)\}$. Since logical $\wedge$ is associative, the two sets are obviously the same.

Theorem 2.4: $\pi_1 \leq \pi_2 \Rightarrow \pi_1 + \pi_2 = \pi_2$

Proof: Because $\pi_1 \leq \pi_2$, we have $B_{\pi_1}(s) \subseteq B_{\pi_2}(s)$ for all $s \in S$ [theorem 1.1]. Therefore, in the base case in $\pi_1 + \pi_2$ construction for any s , we have $B_{\pi_1}(s) \cup B_{\pi_2}(s) = B_{\pi_2}(s)$.

Inductively, because other π_2 blocks are disjoint with $B_{\pi_2}(s)$, and by $B_{\pi_1}(s) \subseteq B_{\pi_2}(s)$, they are also disjoint with $B_{\pi_1}(s)$. Hence, structural induction can only come from $B_{\pi_1+\pi_2}(s) \cup \{B \mid B \cap B_{\pi_1+\pi_2}(s) \neq \emptyset, B \in \pi_1\}$. Assume we have $B_{\pi_1}(t)$ and $B_{\pi_1}(t) \cap B_{\pi_1+\pi_2}(s) \neq \emptyset$. Then, there exists $u \in B_{\pi_1}(t)$ and $u \in B_{\pi_2}(s)$. By theorem 1.1, there exists $B_{\pi_2}(t)$ such that $B_{\pi_1}(t) \subseteq B_{\pi_2}(t)$, which makes $u \in B_{\pi_2}(t)$ by $u \in B_{\pi_1}(t)$. This contradicts with $u \in B_{\pi_2}(s)$ as u is in both $B_{\pi_2}(t)$ and $B_{\pi_2}(s)$ which is impossible if $s \neq t$. In case $s = t$, $B_{\pi_1+\pi_2}(s)$ doesn't change.

Therefore, by induction we have $B_{\pi_1+\pi_2}(s) = B_{\pi_2}(s)$ for all s. That is, $\pi_1 + \pi_2 = \pi_2$. $\square$

Theorem 2.5: Partition addition is associative

Proof:

First, we show that the base case is associative. This obviously holds because for all s, $B_{\pi_1}(s) \cup B_{\pi_2}(s) = B_{\pi_2}(s) \cup B_{\pi_1}(s)$.

Inductively, given $B_{\pi_1+\pi_2}(s) = B_{\pi_2+\pi_1}(s)$, it follows immediately that $B_{\pi_1+\pi_2}(s) \cup \{B \mid B \cap B_{\pi_1+\pi_2}(s) \neq \emptyset, B \in \pi_1 \cup \pi_2\} = B_{\pi_2+\pi_1}(s) \cup \{B \mid B \cap B_{\pi_2+\pi_1}(s) \neq \emptyset, B \in \pi_1 \cup \pi_2\}$. $\square$

Properties 2.1: Given three partitions π_1, π_2 and τ such that $\pi_1 \geq \tau$ and $\pi_2 \geq \tau$, we have

$$\pi_1 \geq \pi_2 \Leftrightarrow \overline{\pi_1} \geq \overline{\pi_2}$$

Proof: To prove $\overline{\pi_1} \geq \overline{\pi_2}$ is to prove $B_\tau(s) \equiv B_\tau(t)(\overline{\pi_2}) \Rightarrow B_\tau(s) \equiv B_\tau(t)(\overline{\pi_1})$ [theorem 1.1]. It is to prove $s \equiv t(\pi_2) \Rightarrow s \equiv t(\pi_1)$ [definition]. This follows immediately from $\pi_1 \geq \pi_2$ [theorem 1.1]. The inverse is similar. $\square$

$$\overline{\pi_1 \cdot \pi_2} = \overline{\pi_1} \cdot \overline{\pi_2}$$

($\overline{\pi_1 \cdot \pi_2} \subseteq \overline{\pi_1} \cdot \overline{\pi_2}$) Suppose there exists $B_{\overline{\pi_1 \cdot \pi_2}}$ in $\overline{\pi_1 \cdot \pi_2}$ and for all blocks $B_{\overline{\pi_1} \cdot \overline{\pi_2}}$ in $\overline{\pi_1} \cdot \overline{\pi_2}$, $B_{\overline{\pi_1 \cdot \pi_2}} \nsubseteq B_{\overline{\pi_1} \cdot \overline{\pi_2}}$. That is, there exists a $B_{\tau 0}$ such that $B_{\tau 0} \in B_{\overline{\pi_1 \cdot \pi_2}}$ and $B_{\tau 0} \notin B_{\overline{\pi_1} \cdot \overline{\pi_2}}$. However, generally, for all $B_{\overline{\pi_1 \cdot \pi_2}}$, there exists a $B_{\overline{\pi_1} \cdot \overline{\pi_2}}$ where there exists B_τ that is in both blocks. Hence, we have $B_\tau \equiv B_{\tau 0}(\overline{\pi_1 \cdot \pi_2})$ and $B_\tau \neq B_{\tau 0}(\overline{\pi_1} \cdot \overline{\pi_2})$.

Let $B_\tau = B_\tau(r)$ and $B_{\tau 0} = B_{\tau 0}(s)$ where $r \neq s(\tau)$. We have $r \equiv s(\pi_1 \cdot \pi_2)$ and ($B_\tau(r) \neq B_\tau(s)(\overline{\pi_1})$ or $B_\tau(r) \neq B_\tau(s)(\overline{\pi_1})$). Further expanding the expression we arrive at a contradiction.

The inverse is similar to prove.

$$\overline{\pi_1 + \pi_2} = \overline{\pi_1} + \overline{\pi_2}$$

Use proof by contradiction similar to above. $\square$

Lattice

Example 3.1: The set of all partitions of S is a partially ordered set under $\leq$ of partitions.

Justification: First we know $\leq$ is a surjective function [corollary 1.1]. Antisymmetry is arrived by that if we have function $\leq$ and $\geq$ (i.e. its inverse), we establish a surjection with an inverse which is a one-to-one correspondence, which means $=$. Transitivity is arrived by functional composition. Reflexivity is trivial. $\square$

Lemma 3.1: When l.u.b/g.l.b exists, it is unique.

Proof:

(l.u.b.) Suppose there exist two distinct l.u.b. s_1, s_2. According to the defintion, for all $s' \geq t$, $s' \geq s_1$. Because s_2 is an $l.u.b.$, $s_2 \geq t$. Plus the previous result, we have $s_2 \geq s_1$. Similarly, we can derive $s_1 \geq s_2$. Yet recall $\ge $ is antisymmetric, so $s_1 \geq s_2, s_2 \geq s_1$ implies $s_1 = s_2$, a contradiction to the hypothesis they are distinct.

(g.l.b) Proof is similar. $\square$

Theorem 3.1: In a lattice, every non-empty subset has a unique l.u.b. and g.l.b.

Proof:

(existence) The base case is a set consists of only two elements, where there is an l.u.b. and g.l.b. according to the definition.

Inductively, assume a set S has an l.u.b. r by ind. hyp., and it has a successor $S' = S \cup \{s\}$. Because L is a lattice, we can establish t as the l.u.b. of r and s. In this case, t is an l.u.b. for S', and the induction holds. Why? Consider any upper bound of S' v. $v \geq r$ because r is the l.u.b. of S. Also, $v \geq s$ simply for $s \in S'$. It follows that we have $v \geq t$ since t is the l.u.b of r and s. Because v is the upper bound of S' and $v \geq t$, we have $l.u.b.(S') = t$.

Proof for g.l.b is similar.

(uniqueness) Lemma 3.1 + induction. $\square$

Example 3.2: The set of all partitions of S is a lattice such that

$$g.l.b.(\pi_1, \pi_2) = \pi_1 \cdot \pi_2$$
$$l.u.b.(\pi_1, \pi_2) = \pi_1 + \pi_2$$

Justification: For g.l.b., need to show that for all $\pi_0 \leq \pi_1$ and $\pi_0 \leq \pi_2$, $\pi_0 \leq \pi_1 \cdot \pi_2$. Suppose there exists π_0 such that $\pi_0 \leq \pi_1$, $\pi_0 \leq \pi_2$, and $\pi_0 \geq \pi_1 \cdot \pi_2$ ($\pi_0 \neq \pi_1 \cdot \pi_2$). Because $\pi_0 \leq \pi_1$ and $\pi_0 \leq \pi_2$, we have $\pi_0 \cdot \pi_1 = \pi_0$, $\pi_0 \cdot \pi_2 = \pi_0$, and thus $(\pi_0 \cdot \pi_1) \cdot \pi_2 = \pi_0$. Since $\pi_0 \geq \pi_1 \cdot \pi_2$, we also have $\pi_0 \cdot (\pi_1 \cdot \pi_2) = \pi_1 \cdot \pi_2$. Because $[\cdot]$ is associative, $\pi_0 = \pi_1 \cdot \pi_2$, which produces a contradiction.

For l.u.b., justification is similar. $\square$

Algebraic definition of lattice

Let triplet $L = (S, \cdot, +)$ where $[\cdot]$ and $[+]$ are both idempotent, communicative, associative, and that $x \cdot (x + y) = x$ plus $x + (x \cdot y) = x$ (absorptive). Next, we define

$$x \leq y \Leftrightarrow x \cdot y = x$$

. Then, $(S, \leq)$ is a lattice and

$$g.l.b.(x, y) = x \cdot y$$
$$l.u.b.(x, y) = x + y$$

Justification:

($x \cdot y$ is indeed g.l.b.) We need to show that for all $s \leq x$ and $s \leq y$, $s \leq x \cdot y$.

Because $s \leq x$ (implying $s \cdot x = s$) and $s \cdot s = s$, $s \cdot x = s \cdot s$ by equality. Also because $s \leq y$ (implying $s \cdot y = s$) and $s \cdot s = s$, $(s \cdot s) \cdot y = s$ by substitution. Combining two results, we have $(s \cdot x) \cdot y = s$, which is equivalent to $s \cdot (x \cdot y) = s$. Hence $s \leq x \cdot y$ followed from definition.

($x + y$ is indeed $l.u.b.$) We need to show that for all $s \geq x$ and $s \geq y$, $s \geq x + y$.

By absorption, we have $s = s + (s \cdot x)$. Applying the same rule again, we have $s = s + (s \cdot y) + (s \cdot x)$. Hence, $s \cdot [(s \cdot x) + (s \cdot y)] = [s + (s \cdot x) + (s \cdot y)][(s \cdot x) + (s \cdot y)]$ by substituting previous result, which is equal to $(s \cdot x) + (s \cdot y)$ by absorption. Substitute $s \cdot x = x$ and $s \cdot y = y$ (since $s \geq x$ and $s \geq y$), we have $s \cdot (x + y) = x + y$, which means $s \geq x + y$. $\square$

Theorem 3.2: In a lattice $x \leq y \Leftrightarrow x + y = y$.

Proof:

($\Rightarrow$) According to the definition $x \leq y \Leftrightarrow x \cdot y = x$, which implies $x \cdot y + y = x + y$. According to distributive and absorptive rule we have $y = x + y$.

($\Leftarrow$) Because $x + y$ is the l.u.b. of x, y, it follows that $x \leq x + y$. Because $x + y = y$, we have $x \leq y$. $\square$

Theorem 3.3: In a lattice $L = (S, \cdot, +)$,

$$\begin{gathered} x_1 \leq x_2 \\ y_1 \leq y_2 \Rightarrow x_1 \cdot y_1 \leq x_2 \cdot y_2 \\ x_1 + y_1 \leq x_2 + y_2 \end{gathered}$$

Proof:

($\Rightarrow x_1 \cdot y_1 \leq x_2 \cdot y_2$) Because $x_1 \leq x_2, y_1 \leq y_2$, $x_1 \cdot x_2 = x_1, y_1 \cdot y_2 = y_1$. Hence, $x_1 \cdot y_1 = (x_1 \cdot x_2) \cdot (y_1 \cdot y_2)$ by substitution, which equals to $(x_1 \cdot y_1) \cdot (x_2 \cdot y_2)$. If follows by definition that $x_1 \cdot y_1 \leq x_2 \cdot y_2$.

($\Rightarrow x_1 + y_1 \leq x_2 + y_2$) case is similar to above. $\square$

Theorem 3.4: In a distributive lattice, the two distributive laws are logically equivalent.

Proof:

($\Rightarrow$) Because $[\cdot]$ is distributive, $(x + y) \cdot (x + z) = [(x + y) \cdot x] + [(x + y) \cdot z] = (x \cdot x) + (x \cdot y) + (x \cdot z) + (y \cdot z)$. By idempotent and absorption, it simplifies to $x + (y \cdot z)$.

($\Leftarrow$) Because $[+]$ is distributive, $(x \cdot y) + (x \cdot z) = [(x \cdot y) + x] \cdot [(x \cdot y) + z] = x \cdot [(x + z) \cdot (y + z)]$, which simplifies to $x \cdot (y + z)$. $\square$

Theorem 3.5: In a distributive lattice, for any x, there can exist at most one y such that $x \cdot y = 0$ and $x + y = I$ (y is called the complement of x).

Proof:

Suppose we have $y_1 \neq y_2$ but both satisfy the two conditions above. Since $x \cdot y_1 = 0, x \cdot y_2 = 0$ and that $0 + 0 = 0$, we have $x \cdot y_1 + x \cdot y_2 = 0$. Because the lattice is distributive, this implies $x \cdot (y_1 + y_2) = 0$, which inductively says $x \cdot I = 0$. Since for all x, $x \cdot I = x$, it must be that $x = 0$. However, due to $x + y = I, 0 + y = I$, and it must be that $y = I$ which is unique. Hence we arrive at a contradiction. $\square$