Abstract Interpretation

枫聆

2021 年 4 月 11 日

目录

Motivation

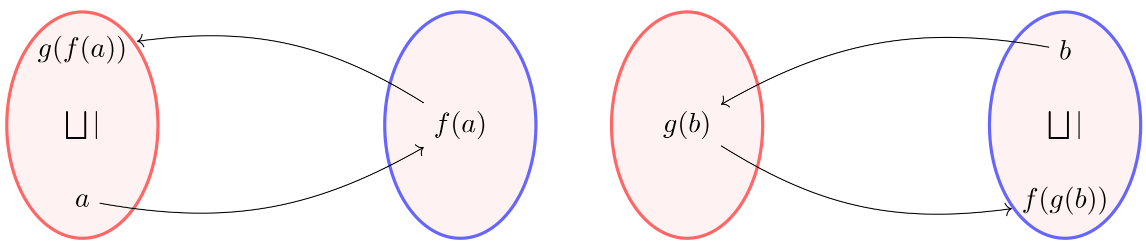
实际分析 domain 太复杂，也许这个实际分析 domain 满足一些不错的性质比如 ACC 等等，但是还是掩盖不了它过于复杂. 所以我们尝试使用某个抽象的 domain 来代替分析，这个抽象的 domain 要比实际分析的 domain 更小，我们分析起来更加得心应手，但是问题是如何构造这个抽象的 domain? 它分析出来的结果是否可以作为真的 truth? 它的结果能在多大程度上说明一些问题? 后期我们是否可以考虑优化抽象的 domain 来让结果更好一点?

Galois connections

关于 galois connection 我们通常可以看到两个定义，下面我来说明两个定义是等价，也就是说可以从任意一个推出另外一个.

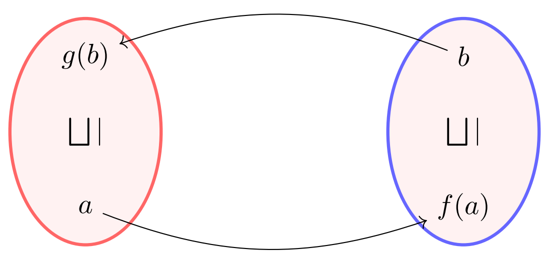
Definition 2.1. nlab 上的定义更贴近 adjunction 的味道 Given posets A and B, a Galois connection between A and B is a pair of order-preversing functions $f\colon A \to B$ and $g\colon B \to A$ such that $a \le g(f(a))$ and $b \ge f(g(b))$ for all $a \in A$, $b \in B$.

注意这里的 order-preversing，最原始的定义用的是 order-reversing，导致我在这里弄出了一些矛盾.



Proposition 2.2. Given posets A and B, a pair of order-preversing functions $f\colon A \to B$ and $g\colon B \to A$ is a Galois connection between A and B if and only if, for all $a \in A$, $b \in B$, we have

$$f(a) \le b \text{ if and only if } a \le g(b).$$



证明. ($\Rightarrow$). 前提 (f, g) 是一个 galois connection，给定 $a \in A$, $b \in B$. 若 $f(a) \le b$, 两边同时 apply g, 有 $g(f(a)) \le g(b)$，同时有 $a \le g(f(a))$. 那么 $a \le g(b)$. 若 $a \le g(b)$，同理可以得到 $f(a) \le b$.

($\Leftarrow$). 前提 (f, g) 满足 $f(a) \le b$ if and only if $a \le g(b)$. 我们直接取 $b = f(a)$, 那么 $f(a) \le f(b)$ 当且仅当 $a \le g(f(a))$. 同理直接取 $a = g(b)$，那么 $g(b) \le g(b)$ 当且仅当 $f(g(a)) \le b$. □

关于 adjunction 的东西 $fg \to id$ 和 $gf \to id$, 这个箭头是一个 natural transform, 至于更细的东西要去看看 category theory 了! PAAA 上说 f 和 g 互为 “weak inverse”，看起来也是比较形象啊！所以有下面的一个命题.

Proposition 2.3. weak inverse For galois connection (f, g), we have the equations

$$f \circ g \circ f = f$$
$$g \circ f \circ g = g.$$

证明. (1).

$$\begin{aligned} a \le g(f(a)) \Rightarrow \quad & f(a) \le f[g(f(a))] \quad && f \circ (g \circ f) \\ f(a) \le f(a) \Rightarrow \quad & f \circ g(f(a))) \le f(a) \quad && (f \circ g) \circ f, \end{aligned}$$

所以 $f \circ g \circ f = f$. 同理可证第二个式子. □

Proposition 2.4. Galois connection 引发的 semilattice homomorphism For a Galois connection (f, g) of join semlattice A and B, f preserves finite join:

1. $f(\perp) = \perp$;

2. $f(x \vee y) = f(x) \vee f(y)$.

啧啧, 没想到啊 galois connection 竟然弄了一个 semilattice homomorphism 出来, 突然想找一下 characterization of semilattice homomorphism.

证明. (1) 由于 B 上的 $\perp$ 的性质, 有 $f(\perp) \ge \perp$. 反过来由于 A 上的 $\perp$ 性质, 有 $g(\perp) \ge \perp$, 再用一下 galois connection 的性质, 有 $f(\perp) \le \perp$. 综上两边夹, 所以 $f(\perp) = \perp$.

(2) 由于 f 是 monotone, 有 $f(x) \le f(x \vee y)$ 和 $f(x) \le f(x \vee y)$, 所以 $f(x) \vee f(y) \le f(x \vee y)$. 最关键的是证明 $f(x \vee y) \le f(x) \vee f(y)$. 由于 galois connection, 有 $x \le g(f(x))$, 再由 g 是 monotone, 有 $x \le g(f(x) \vee f(y))$. 同理也有 $y \le g(f(x) \vee f(y))$, 那么

$$x \vee y \le g(f(x) \vee f(y))$$

再用一下 galois connection, 就有 $f(x \vee y) \le f(x) \vee f(y)$. 综上两边夹, 所以 $f(x \vee y) = f(x) \vee f(y)$. □

Inducing along the Concretisation Function

Definition 2.5. We shall say that the sequence $(x_1\nabla\cdots\nabla x_n)_n$ eventually stabilises whenever there is a number N such that $x_1\nabla\cdots\nabla x_n = x_1\nabla\cdots\nabla x_n\nabla x_{n+1}$ for all $n > N$.

这个 ∇ 表示 widening，这个序列第 n 个元素是 $x_1\nabla\cdots\nabla x_n$，最终会趋于稳定.

Definition 2.6. An operator $\nabla\colon D\times D\to D$ is a strong widening whenever

- $x_1\nabla x_2 \geq x_1 \vee x_2$ holds for all $x_1, x_2 \in D$ and
- the sequence $(x_1\nabla\cdots\nabla x_n)_n$ eventually stabilises for all choices of sequence $x_1, x_2, \cdots$.

widening 弄了一个 upper bound 出来，这个 upper bound 不需要是确界.

Proposition 2.7. 任意次 widening 操作 upper bound 的性质依然保留 If ∇ is a strong widening then

$$x_1\nabla\cdots\nabla x_n \leq x_1\nabla\cdots\nabla x_n\nabla x_{n+1}$$

for all $n > 0$.

证明. 当 $n = 1$ 时

$$x_1 \leq x_1\nabla x_2.$$

这是显然地，假设对任意的 $n = k$ 有 $x_1\nabla\cdots\nabla x_k \leq x_1\nabla\cdots\nabla x_k\nabla x_{k+1}$ 成立，那么当 $n = k+1$ 时

$$\begin{aligned}(x_1\nabla\cdots\nabla x_k\nabla x_{k+1})\nabla x_{k+2} &\geq (x_1\nabla\cdots\nabla x_k\nabla x_{k+1}) \vee x_{k+2}\\ &\geq x_1\nabla\cdots\nabla x_k\nabla x_{k+1}.\end{aligned}$$

所以原式在任意 $n > 0$ 时成立. □

Proposition 2.8. If D satisfies the ACC then the join operation $\vee$ is a strong widening.

证明. 这太显然了，简直 trivial，ACC 在这里保证了任意非空集合都有最大元素，那么它们的 join 肯定不会超过它，也就是 eventually stabilises. □

Definition 2.9. widening operation 的构造 Given galois connection pair (f, g) of A between B, we defined widening operation as follows

$$x\nabla y = g(f(x) \vee f(y))$$

where $x, y \in A$.

Proposition 2.10. strong widening operation Given galois connection pair (f, g) of A between B and B statifies the ACC then ∇ defined above is a strong widening.

证明. (1) 根据 galois connection reduce 出来的 semilattice homomorphism，有 $f(x \vee y) = f(x) \vee f(y)$，再根据 galois connection 的 definition，有

$$x \vee y \leq g(f(x \vee y)) = x \nabla y.$$

(2) 这里需要额外证明 $x_1 \nabla \cdots \nabla x_n = g(f(x_1) \vee \cdots \vee f(x_n))$，由于 B 是满足 ACC 的，所以存在 $f(x_1) \vee \cdots \vee f(x_n) \leq f(x_m)$，即 $x_1 \nabla \cdots \nabla x_n \leq g(f(x_m))$，那么只要 $n > m - 1$ 就有 $x_1 \nabla \cdots \nabla x_n \leq x_1 \nabla \cdots \nabla x_n \nabla x_{n+1}$ 成立. 所以 $(x_1 \nabla \cdots \nabla x_n)_n$ eventually stabilises. $\square$