Abstract Interpretation

枫聆

2021 年 10 月 22 日

目录

Motivation

单调分析框架的诞生让做程序分析的人可以构造一个精准的，数学形式化的分析. 在这个框架下，我们需要一个 lattice domain，每个 instruction 相关联的 transfer functuons 和一个初始的状态. 几乎先有的程序分析手法都可以总结到这个单调分析框架上.

那么抽象解释可以理解为在单调分析框架上又迈出了一步. 我们经常的设计分析思路：开始从一个简单的分析开始，分析结果的正确性可以很容易得到证明. 这里的分析是指 collecting semantics，即从程序的语义里面收集我们想要的信息. 最开始的分析一般来说，我们的想法是非常的理想导致它的可行性或者可计算性是比较难处理的或者说根本不可能处理，因为有可能我们关注的 property 所在 lattice 对应的 underlying set 的基数是比较大的，或者不满足一些良好的性质例如 ACC. 因此我们尝试使用近似计算的方法，把 property 所在的 lattice 变小，这个过程可能是一个迭代的过程，直到我们最终可以计算为止或者达到一个理想的效果. 而抽象解释就是提供这样一种系统的方法来帮助我们.

Correctness Relations

Definition 2.1. (Correctness relations). A relation $R \subseteq V \times L$ is said to be a correctness relation iff it satifies the following two conditions:

1. $\forall v \in V, l_1, l_2 \in L,\ (v \mathcal{R} l_1)$ and $(l_1 \le l_2) \to (v \mathcal{R} l_2)$;
2. $\forall v, \forall L' \subseteq L,\ (\forall l \in L',\ (v \mathcal{R} l)) \to v \mathcal{R} (\bigwedge L')$.

这里 V 表示 concrete values，L 表示 abstract values 构成的 lattice. $v \mathcal{R} l_1$ 表示 l_1 是 v 的一个 approximation.

用自然语言来描述就是 (1) 若 v 对应某个 l_1，那么对于 l_1 的一个 upper approximation l_2，有 $v \in l_2$. (2) 若 v 同时对应多个 abstract values，这里应该是一个 and 的关系，那么 v 可以对应它们的一个 greatest lower bound.

Lemma 2.2. If $\mathcal{R} \subseteq V \times L$ is a correctness relation, then

$$
\begin{aligned}
&v \mathcal{R} \top \\
&(v \mathcal{R} l_1) \text{ and } (v \mathcal{R} l_2) \to v \mathcal{R} (l_1 \wedge l_2) \\
&(v \mathcal{R} l_1) \text{ or } (v \mathcal{R} l_2) \to v \mathcal{R} (l_1 \vee l_2)
\end{aligned}
$$

前面简单的描述了一下 correctness relation 操作含义，但是 correctness relation 中依然模糊是它里面的 lattice 到底在刻画一个怎样东西？我们的分析中为什么要引入 lattice？为了让这个 lattice is reasonable，我们来具体定义这个 lattice 的 meet 和 join 操作的内在含义.

Definition 2.3. we need the meet and the join operator in order to combine abstract values:

1. If a value is described by both l_1 and l_2, by combine these two properties, we obtain the more precise information $l_1 \wedge l_2$.
2. If a value is described by either l_1 or l_2, the most precise info that we can infer is $l_1 \vee l_2$.

在上面定义的 operations 的内在含义下，smaller 代表更精准，bigger 代表更安全，更安全就是指考虑的更全面，不会丢掉信息而造成一些潜在的问题. $\wedge$ 等价于逻辑连词的 and，$\vee$ 等价于逻辑连词的 or. 在实际分析的过程中 $\wedge$ 和 $\vee$ 这两个 operations 就要针对我们关注的 properties 来具体定义，但是它的最本质内在含义是每次都是尽可能在不丢失精确度的可能下，去尽可能的提高结果本身的精确度.

Annotation 2.4. 如何取证明一个分析的正确性 To prove the correctness of the analysis, it is sufficient to prove

1. The initial property (abstract state) l_0 is a correct approximation of the initial value (concrete state) v_0 : $v_0 \mathcal{R} l_0$.

2. Each transition preserves the correctness relation

$$\forall v_1, v_2, l_1, l_2, \ (v_1 \rightsquigarrow v_2) \text{ and } (v_1 \mathcal{R} l_1) \text{ and } (f_L(l_1) = l_2) \rightarrow v_2 \mathcal{R} l_2.$$

用自然语言来描述就是你首先要保证初始状态下 correctness relation 的存在，而后在状态传递的过程中这个 correctness relation 依然是保持的，这个过程就关系到两个传递函数 concrete value transfer function 和 abstract value transfer function.

Galois connections

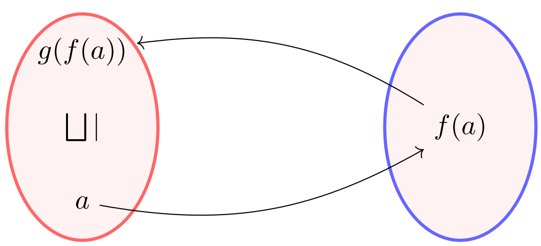
Annotation 3.1. 数学家们经常在思考面临一个场景：有两个“世界”和两个转换函数作为这个两个世界的连接。更甚之，如果其中某个世界中的对象经过转换到另外一个世界中，然后再把这个对象再转换回去，如此往复迭代最终结果是稳定的. 特别地，无论从哪个世界开始，第三次转换的结果和第一次转换的结果是相同的.

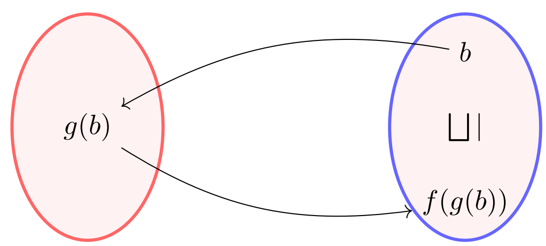
如果这两个世界各自的对象之间着某种自然规律,转换函数在传递过程中遵守这些自然规律 (有点像 structure-preserving). 在类似我们经常碰见的简单或者复杂的场景中, 有一种优雅的方式可以尝试来面对它们–Galois connection。

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 3.2. 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 $a \leq g(f(a))$ and $b \geq f(g(b))$ for all $a \in A$, $b \in B$.

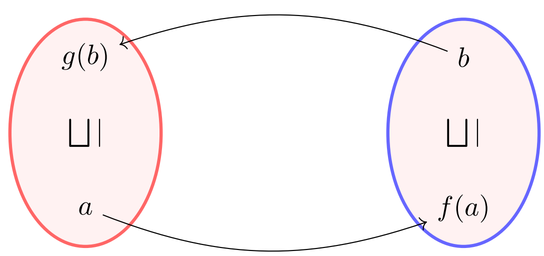
注意这里的 order-preversing，最原始的定义用的是 order-reversing，导致我在这里弄出了一些矛盾.





Proposition 3.3. 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

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



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

$(\Leftarrow)$. 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.

Annotation 3.4. 现在我们尝试把 galois connection 放到抽象解释范畴上，让 lattice A 表示我们原本一个 analysis domain，lattice B 表示一个更抽象的 analysis domain 用来加快我们的分析或者让我们的分析可计算，那么这里 $f\colon A\to B$ 称为abstraction function，$g\colon B\to A$ 称为concretization function.

这里的 f 和 g 都是单调函数意味，原本的实际值之间的关系在 abstract domain 上依然保持，反过来亦然，同时 galois connection 强化的两个条件

1. $a\le g(f(a))$ 表示抽象过程是可能会丢失精度的，但是依然是正确的. 我的理解是把具体的值通过映射放到抽象域里面做运算得到的结果，再映射回来可能比在具体域里面做运算得到的结果要稍微差一点，但是正确性是可以保证的.

2. $b\ge f(g(b)$ 表示具体化的过程不会丢失精度. 本来抽象值，放到具体域里面操作一遍，再映回来是不会丢精度，这也是可以很自然想到的.

如果更细致去刻画一下我自己的 annotation 就是

1. $x,y\in A$
$$x\vee y\le g(f(x)\vee f(y)).$$

2. $x',y'\in B$
$$x'\wedge y'\ge f(g(x')\wedge g(y')).$$

为此我们需要去分别证明 $f(x\vee y)=f(x)\vee f(y)$ 和 $g(x\wedge y)=g(x)\wedge g(y)$.

Annotation 3.5. (关于 lattice 的一些说明) 下述提到的 lattice 都理解为一个 poset，其中 $\wedge = g.l.b(x,y), \vee = l.u.b(x,y)$，semilattice 上的操作一样，不做特殊说明，提到的所有 semilattice 都是 complete 的.

Proposition 3.6. (Galois connection 引发的 semilattice homomorphism) For a Galois connection (f,g) of lattice A and B, f preserves finite join:

1. $f(\perp_A) = \perp_B$;
2. $f(x \vee y) = f(x) \vee f(y)$.

And similarly

1. $g(\top_B) = \top_A$;
2. $g(x \wedge y) = g(x) \wedge g(y)$.

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 $\perp_B$ 的性质，有 $f(\perp_A) \geq \perp_B$. 反过来由于 A 上的 $\perp_A$ 性质 $f \circ g(\perp_B) = \perp_B$，有 $g(\perp_B) \geq \perp_A$，再用一下 galois connection 的性质，有 $f(\perp_A) \leq \perp_B$. 综上两边夹，所以 $f(\perp_A) = \perp_B$.

(2) 由于 f 是 monotone，有 $f(x) \leq f(x \vee y)$ 和 $f(x) \leq f(x \vee y)$，所以 $f(x) \vee f(y) \leq f(x \vee y)$ 是一个 upper bound. 最关键是确界证明 $f(x \vee y) \leq f(x) \vee f(y)$. 由于 galois connection，有 $x \leq g(f(x))$，再由 g 是 monotone，有 $x \leq g(f(x) \vee f(y))$. 同理也有 $y \leq g(f(x) \vee f(y))$，那么

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

再用一下 galois connection，就有 $f(x \vee y) \leq f(x) \vee f(y)$. 综上两边夹，所以 $f(x \vee y) = f(x) \vee f(y)$. 值得关注是 f 和 g 都只是一个 semilattice homomorphism，而且是两种不同操作. 其实我们做分析的时候，也只是使用一个 semilattice，至于是 meet 还是 join 和原本分析过程的方向是有关的. □

Proposition 3.7. (weak inverse) For galois connection (f,g), we have the equations

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

这个命题内在是在说明你把分析结果用 f 和 g 进行迭代是不会改变精度的!

证明.

$$\begin{aligned} f(a) &\leq f \circ (g \circ f(a)) && f \circ (g \circ f) \\ (f \circ g) \circ f(a) &\leq f(a) && (f \circ g) \circ f, \end{aligned}$$

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

Proposition 3.8. (galois connection 的构造 1) If the pair (f, g) is Galois connection of lattice A and B. Then f uniquely determines g by

$$g(b) = \bigvee \{ a \mid f(a) \leq b \}.$$

and g uniquely determines f by

$$f(a) = \bigwedge \{ b \mid a \leq g(b) \}.$$

我个人认为这个性质真的非常好!

证明. 假设给定 join semlattice homomorphism f，我们先来证明上面构造的 g 是符合 galois connection 的 definition. $g(b)$ 单调是显然的. 假设 $c \leq g(d)$，那么

$$f(c) \leq f \circ g(d) \leq d.$$

其中后面这个不等号是因为我们可以用 f 的 semilattice homomorphism 性质展开

$$f \circ g(d) = \bigvee_{x \in \{ a \mid f(a) \leq d \}} f(x) \leq d$$

反过来若 $f(c) \leq d$，那么 f

$$c \leq g \circ f(c) \leq g(d).$$

其中 $g \circ f(c) = \{ a \mid f(a) \leq f(c) \}$，由于 f 是单调的，那么 $\forall a \leq c$.

再证明 g 是唯一的，即若存在 g_1，那么对于任意的 $b \in B$，应该有 $g(b) = g_1(b)$. 因为

$$g(b) \leq (g_1 \circ f) \circ g(b) = g_1 \circ (f \circ g)(b) \leq g_1(b).$$

再把 g 和 g_1 反过来用一遍也可以得到 $g_1(b) \leq g(b)$. 所以有 $g(b) = g_1(b)$. □

Corollary 3.9. (galois connection 的构造 2) If $f\colon A \to B$ is semilattice homomorphism then there exists $g\colon B \to A$ such that (f, g) is a Galois connection of posets (complete semilattice) A and B.

证明. 若 f 是一个 join semilattice homomorphism，那么 f 也是 monotone 的. □

New Analysis: Correctness Relation and Transfer Function

这章讲如何把 analysis function 通过 galois connection 在 analysis domains 之间传递.

Definition 3.10. (新的 correctness relations) The correctness relation $\mathcal{S} \subseteq V \times B$ for the new analysis under Galois connection (f, g) of posets A and B is defined as follows

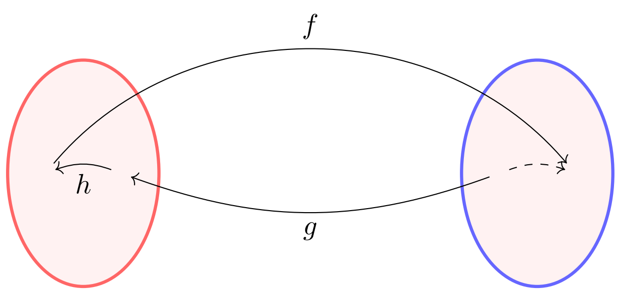
$$v \ \mathcal{S} \ b \iff v \ \mathcal{R} \ g(b).$$

其中的 B 表示新的 analysis domain 或者说是 abstract domain，它还是一个 lattice. 这里是在说 abstract domain 上一个 correctness relations 当且仅当 g 的作用下是 concrete domain 上一个 correctness relation. 其中在 $R \subseteq V \times A$，R 是已知的 correctness relation.

Definition 3.11. (新的传递函数) For the new analysis transfer function, we can choose any function $t_B \colon B \to B$ such that

$$t_B \geq f \circ t_A \circ g.$$

where $t_A \colon A \to A$ is analysis function under A.



但是在实际中我们不会直接通过上面诱导出来的 analysis transfer functions $f \circ t_A \circ g$，因为构造起来太过于繁琐，常常会用一个 t_B 来安全的替换它的使用

定义了新的 correctness relations 和新的 analysis tranfer function，我们现在需要来证明这个 correctness relations 它确实是一个 correctness relation，并且 h' 下保持这个 relation.

Proposition 3.12. $\mathcal{S}$ is a correctness relation.

证明. 给定 $v \ \mathcal{S} \ b_1$ 和 $b_1 \leq b_2$，证明 $v \ \mathcal{S} \ b_2$. 由于 g 是单调的，那么有 $g(b_1) \leq g(b_2)$，再由新定义的 B 上的 correctness relation $v \ \mathcal{R} \ g(b_1)$ 配合已知 A 上的 correctness relation $V \times A$，从而也有 $v \ \mathcal{R} \ g(b_2)$，因此最终得到 $v \ \mathcal{S} \ b_2$.

给定 $v \in V$，设 $B' = \{b \in B \mid v \ \mathcal{S} \ b\}$，证明 $v \ \mathcal{S} \ (\bigwedge B')$. 根据新的 correctness relation 定义，对任意的 $b \in B'$ 都有 $v \ \mathcal{R} \ g(b)$，那么再由 A 上的 correctness relations 有 $v \ \mathcal{R} \ (\bigwedge g(b))$，又因为 g 是一个 meet semilattice homomorphism，那么在这里有 $v \ \mathcal{R} \ g(\bigwedge B')$，即 $v \ \mathcal{S} \ (\bigwedge B')$. $\square$

Lemma 3.13. (新传递函数是 safe 的)

$$g(t_B(a)) \geq t_A(g(a)).$$

证明.

$$g(t_B(a)) \geq (g \circ f) \circ (t_A(g(a))) \geq t_A(g(a)).$$

□

Proposition 3.14. (correctness relations 在新传递函数作用下保持)

$$\forall v_1, v_2, b_1, b_2,\ (v_1 \rightsquigarrow v_2) \text{ and } (v_1\ \mathcal{S}\ b_1) \text{ and } (t_B(b_1) = b_2) \rightarrow v_2\ \mathcal{S}\ b_2.$$

证明. 由上面的 lemma 有

$$g(b_2) \geq t_A(g(b_1))$$

所以 $v_2\ \mathcal{R}\ g(b_2)$，即 $v_2\ \mathcal{R}\ b_2$. □

Annotation 3.15. 可以看到 Galois connection 确实很多的优美的性质，但是想一想实际中我们可能做到这样吗？是否有必要一定将新的 analysis domain 和原来的 domain 构造成一个 Galois connection?

想象两个 analysis domain，都可以很好符合 lattice 代数结构，并且这两个 lattice A, B 还要是 complete，通常我们也只考虑 finite lattice. Galois connection 的存在系统地在 t_A 的基础上诱导出了新的 tranfer analysis function t_B，而且证明了新构造的 correctness relation 是正确的，这就是 Galois connection 起到的重要作用. 我们来具体分析一下在证明它们的过程中哪些是 Galois connection 导致的直接原因.

在证明新的 correctness relation 的时候，第一个条件不需要那么强的条件，只需要 g 单调就行，而第二个条件需要 g 的 meet semilattice homomorphism. 而在证明新的 tranfer analysis function 保持 correctness relations 过程中需要用到 $g \circ f \geq \mathrm{id}_A$，这个条件也算比较强. 在仔细去分析这些条件的时候，我们就可以感受到我们最确切是需要什么. 那么我们反过来问 Galois connection 在这里是不是太强了一些?

Salcianu 在论文 [1] 里面提到可以尝试去掉 correctness relations 的第二个条件，把第二个条件去掉之后我们就不需要 g 保持 semilattice homomorphism 这么强的条件，为什么可以这样做呢？我们考虑新的 abstract analysis domain，实际上它里面的元素和原来的 domain 是联系比较紧密，并且它们之间是可以天然保持我们感兴趣的关系的，例如把 $\mathbb{Z}$ 中的某个数映射到某个包含它的区间，区间和区间之间的 partial order 我们用区间包含来表示 (如果区间 A 可以盖住 B，那么 $B \leq A$)，在对应的 lattice 上，如果一个小区间可以盖住某个值，那么包含这个小区间更大的区间一定也是盖住这个值的. 那么现在来回答 Galois connection 是不是太强了这个问题，我答案确实是太强了，如果站在我们要去证明一个分析的正确性这个命题而言，它是一个充分条件，而不是必要条件.

前面关于 Galois connection 构造性命题中，我们在已知一个 semilattice homomorphism 的情况下，就可以去构造另外一个方向的映射，站在分析的角度而言，我们确实经常有一个 semilattice homomorphism 介于从 concrete domain 到 abstract domain，但是通常是没有必要把从 abstract domain 到 concrete domain 符合 Galois connection 的映射给构造出来，这也就是上面我们提到的，g 不需要保持 semilattice homomorphism 的性质. 但是为了证明新分析过程的正确性我们还是需要 g 是 monotone 并且 $g \circ f \geq \mathrm{id}_A$.

Fixed Point Computation Issues

在单调框架下，我们去计算一个分析结果的时候，最后得到的结果是当前 analysis transfer function 的一个不动点，为什么结果会收敛于某个不动点？当我们 analysis domain 限定为一个 complete lattice，它有一个很好判定性质: 一个 lattice $\mathcal{L}$ 是 complete 的当且仅所有的 order-preserving map $f: \mathcal{L} \to \mathcal{L}$ 都有一个不动点. 并且考虑我们在分析的过程做，中间结果通常是一个 ascending chain 或者 descending chain，这区别于我们从 $\perp$ 开始分析或者从 $\top$. 这里假设我们做分析过程是一个 descending chain，我们希望它最后会下降到一个值之后就稳定了，这一条件我们称为 descending chain condition，简称 DCC，形式化的描述即为: 设中间分析结果序列为 $(f^i(I))_n$，其中 $I = \top, f^0(I) = I$，该序列满足 descending chain，即 $f^{i+1}(I) \leq f^i(I)$，若该序列满足 DCC 则存在一个 N，使得 $n > N$ 时都有 $f(f^n(I)) = f^n(I)$. 设 complete lattice 在 f 上的某个不动点为 u，即 $f(u) = u$，如果我们的 descend chain 刚好 reach 到这个 u，显然我们的分析就停止了，但是 reach 不到跳过了或者在前面还有一个不动点该怎么？因此如果要用 complete lattice 这个性质兜底，就需要好好思考一下这个 f 除了 monotone 之外还需要保持哪些性质?

顺着上面的思路，我们构造了一个单调的 analysis transfer function，并且满足 $f^{i+1}(I) \leq f^i(I)$，那么如何判定它是不是 DCC 的呢？这里有个 trival 的充分条件，若 $(f^i(I))_n$ 中的每一个元素都是 join irreducible(刻画了 lattice 是一条直线)，那么它从 $\perp$ 开始一定就会碰到不动点，并且这个不动点是最大的不动点 gfp. 其实前面一直都在考虑一般情况，通常情况下我们的 analysis domain 是 finite，所以不管是 ascending chain 和 descending chain 终于都会收敛，而 finite lattice 也是一个天然的 complete lattice.

最后我们假设有 DCC 或者 ACC 之后，但是在 analysis domain 不是 finite 的时候，或者基数比较大的时候，如何快速保证 ascending chain 或者 descending chian 收敛呢？所以由此提出了 widening 和 narrowing 的概念，来加快计算不动点过程中收敛的速度. 如果计算中间过程是一个 ascending chain，那么 widening 可以让计算过程快速收敛，并且计算得到的结果是 lfp 的一个 upper approximation. 而 narrowing 就是在这个 upper approximation 的基础上，再去构造一个 safe 的降链去二次逼近 lfp.

Basic Fixed Points Notions

Definition 4.1. Given a order-preserving map $f\colon \mathcal{L}\to\mathcal{L}$ on a complete lattice $\mathcal{L}$.

1. $x\in\mathcal{L}$ is a fixed point for f iff $f(x)=x$ and $\mathrm{Fix}(f)=\{\,x\mid f(x)=x\,\}$ denote the set of fixed points;
2. f is reductive at $x\in\mathcal{L}$ iff $f(x)\leq x$ and $\mathrm{Red}(f)=\{\,x\mid f(x)\leq x\,\}$ denote the set of elements upon which f is reductive;
3. f is extensive at $x\in\mathcal{L}$ iff $f(x)\geq x$ and $\mathrm{Ext}(f)=\{\,x\mid f(x)\geq x\,\}$ denote the set of elements upon which f is extensive.

Lemma 4.2.

$$\mathrm{Fix}(f)=\mathrm{Red}(f)\cap\mathrm{Ext}(f).$$

Definition 4.3. Given a order-preserving map $f\colon \mathcal{L}\to\mathcal{L}$ on a complete lattice $\mathcal{L}$.

$$\bigwedge\mathrm{Fix}(f)=\mathrm{lfp}(f)$$
$$\bigvee\mathrm{Fix}(f)=\mathrm{gfp}(f)$$

证明. 只要证明下面这个 lemma，就证明了当且这个命题. □

Lemma 4.4.

$$\bigwedge\mathrm{Fix}(f)=\bigwedge\mathrm{Red}(f)$$
$$\bigvee\mathrm{Fix}(f)=\bigvee\mathrm{Ext}(f)$$

证明. 在我的 lattice notes 中的 complete lattice 一节中的 Knaster–Tarski theorem 证明的开头里面证明了 $\bigvee\mathrm{Ext}(f)=\bigvee\mathrm{Fix}(f)$. □

Lemma 4.5. Let η be an ordinal number with cardinality greater than $|\mathcal{L}|$, let $\xi=\eta+1$. Define $g\colon \xi\to\mathcal{L}$ by transfinite recurison as $g(0)=\perp$, and

$$g(\beta)=\bigvee\{\,f(g(\alpha))\mid\alpha<\beta\,\}.$$

Then for all $e\in\mathrm{Fix}(f)$, $g(\alpha)\leq e$ implies thats

$$g(\alpha+1)=f(g(\alpha))\leq f(e)=e.$$

这是一个非常有趣的 lemma，它可以告诉你 f 是有不动点的，并且帮你构造出 f 的最小不动点.

证明. 我们首先考察 g 的定义，考虑 $\alpha < \beta$，那么有 $g(\alpha) \leq g(\beta)$，这是马上可以从定义的出来的结论. 更甚之，有 $g(\alpha+1) = f(g(\alpha))$，因为 f 是 order-preserving 的，有 $f(g(\beta)) \geq f(g(\alpha))$. 所以 $g(\alpha) \leq e$ 可以改成

$$g(\alpha+1) = f(g(\alpha)) \leq f(e) = e.$$

因此这个结论告诉我们如果能找到某个 α 使得 $g(\alpha) \leq e$，那么对于所有 $\beta > \alpha$，也有 $g(\beta) \leq e$. 我们可以直接选 $\alpha = 0$，并且对任意 e 都有 $g(0) = \perp \leq e$，也就是说对任意的 $\beta \in \xi$ 都有 $g(\beta) \leq \bigwedge \mathrm{Fix}(f)$.

接下来我们证某个 $g(\beta)$ 是 $f(x)$ 的不动点. 由于 ξ 的基数是大于 $\mathcal{L}$ 的基数，因此存在 $\delta, \gamma \in \xi$，使得 $g(\delta) = g(\gamma)$. 假设 $\delta < \gamma$，由于 g 是 monotone，那么对于所有的 $\delta \leq \beta \leq \gamma$ 都有 $g(\delta) = g(\gamma) = g(\beta)$，因此我们总可以选取 β，使得 $\beta + 1$ 也在 δ 和 γ 中间，那么有

$$g(\beta+1) = f(g(\beta)) = g(\beta),$$

结合前述条件，那么这样 $g(\beta)$ 就是我们找到的 least fixpoint. □

Theorem 4.6. Kleene fixed-point theorem Given a order-preserving $f \colon \mathcal{L} \to \mathcal{L}$ on a complete lattice $\mathcal{L}$, then

$$f^{\beta}(\perp) \leq \bigvee \{ f^{\alpha}(\perp) \mid \alpha \in \mathbb{N} \} \leq \mathrm{lfp}(f).$$

证明. 由 Lemma 4.5，这里显然 $g(\alpha) = f^{\alpha}(\perp)$，但是 $\mathbb{N} \leq \xi$，因此这里并不能直接把 lfp 找出来，从而我们只能写成一个不等式. 如果加强 f 使之变成一个 meet homomorphism，那么我们可以直接证明 $\bigvee \{ f^{\alpha}(\perp) \mid \alpha \in \mathbb{N} \}$ 是一个 fixed point，即

$$\bigvee \{ f^{\alpha}(\perp) \mid \alpha \in \mathbb{N} \} = f^{0}(\perp) \cup \bigvee \{ f^{\alpha}(\perp) \mid \alpha \in \mathbb{N}^{+} \} = f\left(\bigvee \{ f^{\alpha}(\perp) \mid \alpha \in \mathbb{N} \} \right),$$

□

Proposition 4.7.

$$\mathrm{glp}(f) \leq \bigwedge \{ f^{\alpha}(\top) \mid \alpha \in \mathbb{N} \} \leq f^{\beta}(\top),$$

证明. 同4.6. □

Widening and Narrowing

Definition 4.8. Widening and narrowing are both an binary opertor, we use $\nabla\colon \mathcal{L}\times\mathcal{L}\to\mathcal{L}$ denote widening and $\Delta\colon \mathcal{L}\times\mathcal{L}\to\mathcal{L}$ denote narrowing.

Definition 4.9. We shall say that the sequence $(x_1\nabla x_2\nabla\cdots\nabla x_n)_n$ eventaully 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 4.10. An operator $\nabla\colon \mathcal{L}\times\mathcal{L}\to\mathcal{L}$ 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 4.11. 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 4.12. If $\mathcal{L}$ 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 4.13. 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 $x, y \in A$.

Lemma 4.14.

$$x_1 \nabla \cdots \nabla x_n = g(f(x_1) \vee \cdots \vee f(x_n)).$$

证明. 用归纳法来证明，当 $n = 2$ 时做为 base 是显然成立的，假设 $n = k$ 时成立，那么当 $n = k + 1$ 时, 有

$$\begin{aligned}(x_1 \nabla \cdots \nabla x_k) \nabla x_{k+1} &= g(f(x_1 \nabla \cdots \nabla x_k) \vee f(x_{k+1})) \\ &= g(f(\underline{g(f(x_1) \vee \cdots \vee f(x_k))}) \vee f(x_{k+1})) \\ &= g(f(g(f(\underline{x_1 \vee \cdots \vee x_k})))) \vee f(x_{k+1}))\end{aligned}$$

前面我们证明过 $f \circ g \circ f = f$, 所以最后有 $g(f(x_1) \vee \cdots \vee f(x_{k+1}))$. □

Proposition 4.15. 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) 由于 B 是满足 ACC 的，对于任意的 $\{(x_1 \nabla \cdots \nabla x_i)\}_{i \in I}$，存在最大元素 $(x_1 \nabla \cdots \nabla x_m)$，因此只要 $n > m - 1$ 就有 $x_1 \nabla \cdots \nabla x_n = x_1 \nabla \cdots \nabla x_n \nabla x_{n+1}$ 成立. 所以 $(x_1 \nabla \cdots \nabla x_n)_n$ eventually stabilises. □

Proposition 4.16. 一般地 strong widening 构造

$$x \nabla y = g(f(x) \nabla' f(y)),$$

if ∇' is a strong widening on B, then ∇ is a strong widening on A.

Definition 4.17. Similarly, An operator $\Delta \colon \mathcal{L} \to \mathcal{L}$ is a strong narrowing operator iff

1. For all $x_1 \leq x_2$, then $x_1 \leq x_1 \Delta x_2 \leq x_2$;
2. The sequence $(x_1 \Delta \cdots \Delta x_n)_n$ eventually stabilises (there is a number N such that $x_1 \Delta \cdots \Delta x_n = x_1 \Delta \cdots \Delta x_n \Delta x_{n+1}$ for all $n > N$) for all choices of sequence $x_1, x_2, \cdots$.

Applying widening and narrowing

我们在定义 widening 和 narrowing 之后，如何应用这两个 binary operator 呢?

Proposition 4.18. (构造 ACC 收敛序列) Given a monotone transfer function $f\colon \mathcal{L}\to\mathcal{L}$ on a complete lattice $\mathcal{L}$, and a strong widening operator ∇ on $\mathcal{L}$, we define the new transfer function as follow

$$f_{\nabla}^{n} = \begin{cases} \perp & \text{if } n = 0 \\ f_{\nabla}^{n-1} & \text{if } n > 0 \text{ and } f(f_{\nabla}^{n-1}) \leq f_{\nabla}^{n-1} \\ f_{\nabla}^{n-1} \nabla f(f_{\nabla}^{n-1}) & \text{otherwise} \end{cases}$$

The $(f_{\nabla}^{n})_n$ evetually stabilizes at value f_{∇}^{m}. i.e., $\forall n > m, f_{\nabla}^{n} = f_{\nabla}^{m}$.

证明. 很显然 $(f_{\nabla}^{n})_n$ 是个升链，假设 $(f_{\nabla}^{n})_n$ 不收敛，那么必有对于任意的 $n > 0$，存在 $k > n$ 有 $f(f_{\nabla}^{k-1}) \not\leq f_{\nabla}^{k-1}$，即有

$$f_{\nabla}^{k} = f_{\nabla}^{k-1} \nabla f(f_{\nabla}^{k-1}) > f_{\nabla}^{k-1}.$$

把所有这样的 $f(k)$ 做一个 widening 操作

$$f_{\nabla}^{k_1} \nabla \cdots \nabla f_{\nabla}^{k_n} > f_{\nabla}^{k_n - 1}.$$

这和 ∇ 是个 strong widening 矛盾，所以原命题得证. $\square$

Lemma 4.19.

$$f_{\nabla}^{m} \geq \operatorname{lfp}(f).$$

证明. 因为 $f_{\nabla}^{n}{}_n$ 最终会收敛于 f_{∇}^{m}，那么肯定当 $n = m$ 时，肯定是满足 $f(f_{\nabla}^{m}) \leq f_{\nabla}^{m}$，因此 $f_{\nabla}^{m} \in \operatorname{Red}(f)$，从而 $f_{\nabla}^{m} \geq \bigwedge \operatorname{Red}$. $\square$

Lemma 4.20.

$$(f^{n}(f_{\nabla}^{m}))_n$$

is a descending chain of elements in $\operatorname{Red}(f)$.

证明. 当 $n = 1$ 时，$f(f_{\nabla}^{m}) \leq f_{\nabla}^{m}$，假设 $n = k$ 时，有 $f^{k}(f_{\nabla}^{m}) \leq f^{k-1}(f_{\nabla}^{m})$ 成立，那么当 $n = k + 1$ 时有

$$f^{k+1}(f_{\nabla}^{m}) = f(f^{k}(f_{\nabla}^{m})) \leq f(f^{k-1}(f_{\nabla}^{m})) = f^{k}(f_{\nabla}^{m}).$$

$\square$

Annotation 4.21. 前面两个 lemma 说明通过 widening 得到结果是 safe 的，它是 lfp 的一个 upper approximation. 并且观察到 $(f^n(f_\nabla^m))_n$ 是一个降链，并且这个链上所有元素在 f 上都是 reductive 的，那么 $(f^n(f_\nabla^m))_n \leq \mathrm{lfp}(f)$，如果按照这个降链再次逼近 lfp 得到的结果也是 safe 的. 但是同样需要考虑逼近的速度，所以进一步提出了 narrowing 的策略，这就是 narrowing 的 motivation.

Proposition 4.22. (构造 DCC 收敛序列二次逼近) Given a monotone transfer function $f\colon \mathcal{L}\to\mathcal{L}$ on a complete lattice $\mathcal{L}$, and a strong narrowing operator ∇ on $\mathcal{L}$, we define the new transfer function as follow

$$f_\Delta^n = \begin{cases} f_\nabla^m & \text{if } n = 0 \\ f_\Delta^{n-1} \Delta f(f_\Delta^{n-1}) & \text{if } n > 0 \end{cases}$$

证明. 首先证明 $f(f_\Delta^{n-1}) \leq f_\Delta^{n-1}$，即 $(f_\Delta^n)_n$ 是一个 descending chain. 当 $n = 0$ 时，有 $f(f_\nabla^m) \leq f_\nabla^m$，假设 $n = k-1$ 有 $f(f_\nabla^{k-1}) \leq f_\nabla^{k-1}$ 成立. 当 $n = k$ 时，有

$$f(f_\Delta^k) = f(f_\Delta^{k-1} \Delta f(f_\Delta^{k-1})) \leq f(f_\Delta^{k-1}) \leq f_\Delta^{k-1} \Delta f(f_\Delta^{k-1}) = f_\Delta^k.$$

那么 $(f_\Delta^n)_n \in \mathrm{Red}(f)$，即若它收敛，它必定收敛于 $\mathrm{lfp}(f)$ 的一个 upper bound，显然在 strong narrowing 的限制下它是收敛的. □

Example 4.23. 在 range analysis 或者 interval analysis 里面，concrete analysis domain 为

$$\mathbf{Interval} = \{\bot\} \cup \{\, [z^-, z^+] \mid z^- \in \mathbb{Z} \cup \{-\infty\}, z^+ \in \mathbb{Z} \cup \{+\infty\}, z^- \leq z^+ \,\}.$$

我们考虑对应的 lattice 代数结构，我们得来定义一下 meet 和 join 两个 operation. 先定义区间之间的包含关系，若 $[x_1, y_1] \subseteq [x_2, y_2]$，那么当且仅当 $x_1 \geq x_2$ 和 $y_1 \leq y_2$. 注意区间的定义有 $x_1 \leq y_1$ 和 $x_2 \leq y_2$. 定义两个区间的并 $[x_1, y_1] \cup [x_2, y_2] = [\min(x_1, x_2), \max(y_1, y_2)]$ 为同时包含两个区间的最小区间. 再定义两个区间的交为 $[x_1, y_1] \cap [x_2, y_2] = [\max(x_1, x_2), \min(y_1, y_2)]$ 两个区间同时包含最大的区间. 注意这两个 operation 我们同时要考虑 $\bot$ 的情况，我在这里省略了. 所以 lattice 上的 meet 对应区间的交，join 对应区间的并，元素之间的 order 为区间的包含.

这个 concrete analysis domain 构成的是一个 infinite lattice，可以想象一个上述不含有 $[-\infty, +\infty]$ 构成的升链，它是不可能收敛的，即不满足 ACC. 所以我们自然的考虑下面的 abstract analysis domain

$$\mathbf{Interval}_K = \{\bot\} \cup \{\, [z^-, z^+] \mid z^- \in K \cup \{-\infty\}, z^+ \in \mathbb{K} \cup \{+\infty\}, z^- \leq z^+ \,\}.$$

其中 K 是一个 finite set，在 K 限制下现在的 analysis domain 是一个 finite lattice. 我们可以定义 **Interval** 和 **Interval**$_K$ 之间的一个 galois connection. 从 **Interval**$_K$ 到 **Interval** 的 g 是比较直接的

$$\begin{aligned} g(\bot) &= \bot \\ g([k^-, k^+]) &= [k^-, k^+] \end{aligned}$$

我们应用一下前面 galois connection 的构造方式来尝试构造一下 f,

$$f(a) = \bigwedge\{\, b \mid a \leq g(b) \,\}.$$

考虑 $a = [z^-, z^+]$，那么

$$f([z^-, z^+]) = [\inf\{\, k \in K \mid k \leq z^- \,\}, \sup\{\, k \in K \mid k \geq z^+ \,\}] = [\lfloor z^- \rfloor, \lceil z^+ \rceil]$$

特别的 $f(\bot) = \bot$. 最后我们定义 widening operation ∇: **Interval** $\times$ **Interval**$\rightarrow$**Interval** 如下

$$\mathrm{int}_1 \nabla_K \mathrm{int}_2 = \begin{cases} \bot & \text{if } \mathrm{int}_1 = \mathrm{int}_2 = \bot \\ [\lfloor z^- \rfloor, \lceil z^+ \rceil] & \text{if } \mathrm{int}_1 = [z^-, z^+], \mathrm{int}_2 = \bot \\ [\lfloor z^- \rfloor, \lceil z^+ \rceil] & \text{if } \mathrm{int}_1 = \bot, \mathrm{int}_2 = [z^-, z^+] \\ [\lfloor z^- \rfloor, \lceil z^+ \rceil] & \text{if } \mathrm{int}_1 = [z_1^-, z_1^+], \mathrm{int}_2 = [z_2^-, z_2^+] \text{ and } z^- = \min(z_1^-, z_2^-), z^+ = \max(z_1^+, z_2^+) \end{cases}$$

这个 widening operator 是直接作用在 concrete analysis domain 上，可以理解为

$$\mathrm{int}_1 \nabla \mathrm{int}_2 = g(f(\mathrm{int}_1) \vee f(\mathrm{int}_2)).$$

呼！终于 make sense 了.

这个 K 是一个 finite set. 例如给定 $K = [-2^3, 2^3 - 1] = [-8, 7]$，给定下面区间包含关系下的升链

$$[0,1],\ [-1,2],\ [-2,4],\ [-4,8],\ [-8,16],\ [-16,32],\ [-32,64]\ \cdots$$

在 $g \circ f$ 的作用下

$$[0,1],\ [-1,2],\ [-2,4],\ [-4,\infty],\ [-8,\infty],\ \mathbb{Z},\ \mathbb{Z}\ \cdots$$

或者你可以尝试两两做下 widening 操作，也会 eventually stabilises.

参考文献

[1] Alexandru Sălcianu (2001) Notes on Abstract Interpretation.