Verifica del Software - Esercizi parte 2

Università degli Studi di Padova

Mirko Bez

19 febbraio 2017

Indice

Esercizio 1

Consegna *Let (α, C, A, γ) be a Galois connection. Prove that:*

(A) γ is injective, $\iff$

(B) $\alpha \circ \gamma = id$ $\iff$

(C) α is surjective.

Svolgimento Alcune definizioni utili:

Definizione 1. *(Galois Connection) (α, C, A, γ) è una Galois connection se:*

1. *A, C sono poset*
2. *$\alpha : C \to A$ monotona*
3. *$\gamma : A \to C$ monotona*
4. *$\forall c \in C.\ c \leq_C \gamma(\alpha(c))$*
5. *$\forall a \in A.\ \alpha(\gamma(a)) \leq_A a$*

Definizione 2. *(Funzione iniettiva) Una funzione $f : X \to Y$ è iniettiva se:*

$$\forall a, b \in X.\ f(a) = f(b) \implies a = b$$

$\boxed{(B) \implies (A)}$ Assumo che valga l'ipotesi (B) ovvero che $\alpha \circ \gamma = id$. Assumo per assurdo che non valga l'ipotesi (A) ovvero che γ non sia iniettiva, quindi:

$$\exists a, b \in A.\ \gamma(a) = \gamma(b) \wedge a \neq b$$

Siano a, b due elementi diversi di A ($a \neq b$) che vengono mappati allo stesso elemento di C, ovvero $\gamma(a) = \gamma(b)$. Essendo $(C, \leq_C)$ un poset, per la riflessività della relazione $\leq_C$, valgono anche le relazioni:

I) $\gamma(a) \leq_C \gamma(b)$

II) $\gamma(b) \leq_C \gamma(a)$

Partendo dalla relazione I) ottengo:

$$\begin{array}{ll} \gamma(a) \leq_C \gamma(b) & \implies \text{per la monotonia di } \alpha \\ \alpha(\gamma(a)) \leq_A \alpha(\gamma(b)) & \implies \text{per l'ipotesi (B)} \\ a \leq_A b & \end{array}$$

Partendo dalla relazione II) ottengo:

$$\begin{array}{ll} \gamma(b) \leq_C \gamma(a) & \implies \text{per la monotonia di } \alpha \\ \alpha(\gamma(b)) \leq_A \alpha(\gamma(a)) & \implies \text{per l'ipotesi (B)} \\ b \leq_A a & \end{array}$$

Siccome valgono al contempo $a \leq_A b$ e $b \leq_A a$ allora per l'antisimmetria del poset $(A, \leq_A)$ $a = b$. Che è in contrasto con l'ipotesi iniziale che $a \neq b$.

$\boxed{(A) \implies (C)}$ Assumo γ iniettiva, ovvero $\forall a, b \in A.\ \gamma(a) = \gamma(b) \implies a = b$. Devo dimostrare che α suriettiva, ovvero:

$$\forall a \in A.\ \exists c \in C.\ \alpha(c) = a$$

Per fare ciò assumo che α sia non suriettiva ovvero

$$\exists a \in A.\ \forall c \in C.\ \alpha(c) \neq a$$

e sia a_0 un elemento tale che $\alpha(c) \neq a_0 \forall c \in C$.

$$\begin{array}{ll} \alpha(\gamma(a_0)) \leq_A a_0 & \text{Siccome è una GC} \\ \gamma(\alpha(\gamma(a_0))) \leq_C \gamma(a_0) & \text{Poichè } \gamma \text{ monotona} \end{array}$$

Inoltre siccome $\gamma(a_0) \in C$ vale

$$\gamma(a_0) \leq \gamma(\alpha(\gamma(a_0)))$$

Quindi unendo i due risultati (per l'antisimmetria di $\leq_C$) ottengo:

$$\begin{array}{ll} \gamma(a_0) = \gamma(\alpha(\gamma(a_0))) & \text{Siccome } \gamma \text{ iniettiva} \\ a_0 = \alpha(\gamma(a_0)) & \text{Contraddizione} \end{array}$$

Avendo ottenuto una contraddizione ottengo che sotto l'assunzione (A) non può esistere un $a_0 \in A$ tale che $\alpha(c) \neq a$ e quindi α è necessariamente suriettiva.

$\boxed{(C) \implies (B)}$ Assumo α suriettiva ovvero:

$$\forall a \in A.\ \exists c \in C.\ \alpha(c) = a$$

Assumo che non valga (B) $\alpha \circ \gamma \neq id$ ovvero:

$$\exists a \in A : \alpha(\gamma(a)) \neq a$$

Sia a_0 tale che $\alpha(\gamma(a_0)) \neq a_0$. Siccome (α, A, C, γ) è una GC vale $\alpha(\gamma(a_0)) \leq a_0$. Dimostrando $a_0 \leq_A \alpha(\gamma(a_0))$ otterrei una contraddizione.

Siccome abbiamo a che fare con una GC (e α, γ totali):

$$\gamma(\alpha(a_0)) \leq_C \gamma(\alpha(\gamma(a_0)))$$

Se γ fosse iniettiva seguirebbe immediatamente il risultato cercato, ovvero $a_0 \leq (\alpha(\gamma(a_0)))$. Dimostro che γ debba per forza essere iniettiva:

TODO: DIMOSTRA INIETTIVITÀ DI γ

Esercizio 2

Consegna *Let C and A be complete lattices and let (α, C, A, γ) be a Galois connection. Prove the following properties:*

1. $\gamma(\alpha(\top_C)) = \top_C$
2. *for any* $a \in A, \gamma(a) = \wedge\{c \in C \mid \alpha(c) \leq_A a\}$
3. *for any* $c_1, c_2 \in C, \alpha(c_1 \vee_C c_2) = \alpha(c_1) \vee_A \alpha(c_2)$
4. *for any* $c \in C, \gamma(\alpha(\gamma(\alpha(c)))) = \gamma(\alpha(c))$

Svolgimento

Esercizio 3

Consegna *Let C and A be complete lattices, (α, C, A, γ) be a Galois insertion, $op : C^2 \to C$ be a monotone concrete operation and $op^a : A_2 \to A$ be a monotone abstract operation. Prove the following equivalence:*

$$\begin{array}{c} \forall (a_1, a_2) \in A^2\ .\ \alpha(op(\gamma(\alpha_1), \gamma(\alpha_2))) \leq_A op^a(a_1, a_2) \\ \iff \\ \forall (c_1, c_2) \in C^2\ .\ op(c_1, c_2) \leq_C \gamma(op^a(\alpha(c_1), \alpha(c_2))) \end{array}$$

Svolgimento

Esercizio 4

Consegna *Let $\langle C, \leq_C \rangle$ be a complete lattice and let $S \subseteq C$ be a subset of C which is meet-closed, that is:*

$$\forall Y \subseteq S. \wedge_C Y \in S$$

Prove that $\langle S, \leq_C \rangle$ can be viewed as an abstract domain of C where the concretization map $\gamma : S \to C$ is the identity.

Svolgimento

Esercizio 5

Consegna *Let C and A be complete lattices, (α, C, A, γ) be a Galois insertion, $f : C \to C$ be a monotone concrete operation and $f^\sharp : A \to A$ be a monotone abstract operation such that: $f \circ \gamma = \gamma \circ f^\sharp$. Prove that $\alpha(gfp(f)) = gfp(f^\sharp)$.*

Svolgimento

Esercizio 6

Consegna *Let C and A be complete lattices, (α, C, A, γ) be a Galois insertion, $f : C \to C$ be a monotone concrete operation and $f^\sharp : A \to A$ be a monotone abstract operation such that: $\alpha \circ f = f^\sharp \circ \alpha$.*

1. *Prove that $\alpha(lfp(f)) = lfp(f^\sharp)$.*
2. *Give a counterexample to the equality $lfp(f) = \gamma(lfp(f^\sharp))$.*

Svolgimento

Esercizio 7

Consegna *Let $(\alpha, \langle A, \leq_A \rangle, \langle \wp(Z), \subseteq \rangle, \gamma)$ be a Galois connection. Let Let $\mathbb{S}^A$, $Var \to A$ and consider the standard pointwise order $\sqsupseteq$ between functions: $s_1^\sharp \sqsubseteq s_2^\sharp$ when for any $x \in Var$, $s_1^\sharp(x) \leq_A s_2^\sharp(x)$. Prove that $(\alpha_s, wp(State), \mathbb{S}^A, \gamma_s)$ is a Galois connection, where:*

- $\alpha_s(T) \triangleq \lambda x.\alpha(\{s(x) | s \in T\})$
- $\gamma_s(s^\sharp) \triangleq \{s \in State | \forall x \in Var.\alpha(\{s(x)\}) \leq_A s^\sharp(x)\}$

Svolgimento

Esercizio 8

Consegna *Consider the following abstract domain of $\langle \wp(\mathbb{Z}, \subseteq) \rangle$*

Svolgimento

Esercizio 9

Svolgimento