Quasi-metric spaces as domains for abstract interpretation

Federico Crazzolara
Dipartimento di Informatica, Università di Pisa
Corso Italia 40, 56125 Pisa, Italy
crazzola@di.unipi.it

Abstract

Metrics and more generally quasi-metrics are well known in literature on domain theory and the semantics of programming languages. In this paper, we consider the role of quasi-metrics in defining abstract interpretations. In fact these allow both to represent a notion of approximation together with the error introduced, and to apply, under suitable conditions, Banach's contraction principle.

Keywords. Abstract interpretation, Galois connection, adjunction, quasi-metric, contraction, approximation space, approximation operator, representation space, program analysis, logic programming.

1 Introduction

The concept of approximation is essential for static analysis of programs, since most interesting properties of programs are undecidable. Abstract interpretation (AI) is a theory for the approximation of the semantics of discrete dynamic systems [4], whose main fields of application are the static analysis of programs and the design of hierarchies of approximated semantics. The classical approach to AI is based essentially on sets equipped with order relations. These relations ensure applicability of fixpoint theorems and represent a notion of approximation between assertions. Indeed in that case $x \sqsubseteq y$ means y approximates x, moreover $\sqsubseteq$ is typically a partial order.

In this paper we study an alternative to the classical framework due to Cousot & Cousot, for designing abstract interpretations of programs. For this purpose we consider metrics. A metric over a set X is a function $d \in X \times X \to \mathbb{R}^+$ that fulfills some properties. The idea is to represent the approximation between two elements x and y, using the value of a metric. A metric may encode not only the concept of approximation between elements of a set, but also the error introduced by the approximation of an element of the set with an other. So it is natural to think of y approximating x whenever the distance between x and y is a non negative real number. The distances contemplated in this paper are usually quasi-metrics rather then metrics: Whenever y approximates x it is not said to hold the inverse. In order to express the fact that x does not approximate y we will say that the distance between y and x is $+\infty$, or intuitively, that the error introduced in the approximation of y by x is not measurable and so corresponds to an indefinite value. By means of quasi-metrics instead of partial orders we construct an AI theory in which the introduced notion of approximation error allows the comparison between different abstractions. In fact we project approximations over a common, totally ordered set, making them always comparable: The closed interval $[0, +\infty]$ (error space).

Typically an AI corresponds to evaluate programs over approximate domains. This consists in solving a suitable recursive equation, representing the semantics of programs, defined on an abstract domain. Thus it is essential to structure domains in a way that the known fixpoint results are applicable. The classical framework for AI considers usually complete lattices as domains and monotonic functions on them, so that Knaster-Tarsky's fixpoint theorem can be applied. On the other hand, Banach's contraction principle is well known to be the major alternative for Knaster-Tarsky's fixpoint theorem. Banach's theorem presumes domains that are (quasi-)metric spaces and contractive functions on them. These two methods are in general not comparable: While Knaster-Tarsky's requires monotonic functions and several fixponts are allowed, Banach's requires contractions and ensures a unique fixpoint. The hypothesis of contraction instead of monotonicity, allows us to overcome problems due to fixpoint semantics based on non monotonic functions, e.g. in the semantics of logic programs with negation: The immediate consequence operator associated with the program is usually not monotonic (see [12, 18]).

To the best of our knowledge, this is the first work which deals with quasi-metrics in AI.

2 Preliminaries

We will assume familiarity with the basic notions of lattice theory (see [11]) and abstract interpretation based on Galois connections (see [4, 5, 6, 7, 8]). As an example of programming language we consider logic programming, therefore we will assume familiarity with it's most important notions (see [2]).

2.1 Basic notation

$\mathbb{N}$ denotes the set of natural numbers, $\mathbb{N}^0$ the set of natural numbers plus zero and $\mathbb{R}^+$ the set of real numbers greater or equal than zero. Let C and D be sets. If $\approx$ is an equivalence relation on C, we denote with $C_{|\approx}$ the set of equivalence classes with respect to $\approx$. The powerset of C is denoted by $\wp(C)$, the set-difference between C and D is denoted by $C \setminus D$. Let f be a mapping on D and $D \subseteq C$, then $f(D) = \{f(x) \mid x \in D\}$, while $f_{|D}$ denotes the function f restricted on D. By $g \circ f$ we denote the function $\forall x \,.\, (g \circ f)(x) = g(f(x))$. f^n denotes, if $n = 0$ the identical mapping and if $n > 0$ the mapping $f^n = f \circ f^{n-1}$. The set D together with a partial order $\sqsubseteq$ is denoted by $\langle D, \sqsubseteq \rangle$. $PRE(I)$ denotes the set of all pre-orders on a set I and $PO(I)$ the set of all partial orders on I.

2.2 Metrics and quasi-metrics

A *metric* on a set X is a mapping $d \in X \times X \to \mathbb{R}^+$ satisfying $\forall x, y, z \in X$:

1. $d(x,x) = 0$ (reflexivity)
2. $d(x,y) = d(y,x)$ (symmetry)
3. $d(x,y) \leq d(x,z) + d(z,y)$ (triangle inequality)
4. $d(x,y) = d(y,x) = 0 \Rightarrow x = y$ (identity of indiscernibles)

(see [20, 21]). If symmetry does not hold, d is said to be a *quasi-metric*. A set X together with a (quasi-)metric d on X is a (quasi)-metric space $\langle X, d\rangle$. Let $A \subseteq X$; the subspace $\langle A, d_{|A}\rangle$ of $\langle X, d\rangle$ is a (quasi-)metric space.

A mapping $f \in \langle X, d_X\rangle \rightarrow \langle Y, d_Y\rangle$ between two (quasi-)metric spaces is said to be non expansive if $\forall x, y \in X \ . \ d_Y(f(x), f(y)) \leq d_X(x, y)$, contractive if there is a real number $c < 1$ such that $\forall x, y \in X \ . \ d_Y(f(x), f(y)) \leq c \cdot d_X(x, y)$, isometric if $\forall x, y \in X \ . \ d_Y(f(x), f(y)) = d_X(x, y)$.

A sequence $(x_n)_{n\in\mathbb{N}}$ of points of a (quasi-)metric space $\langle X, d\rangle$ is Cauchy provided that $\forall \epsilon > 0 \ \exists k \ \forall m, n \geq k \ . \ d(x_m, x_n) \leq \epsilon$. A point $x \in X$ is a (bi-)limit of a sequence $(x_n)_{n\in\mathbb{N}}$ if $\forall \epsilon > 0 \ \exists k \ \forall n \geq k \ . \ d(x_n, x) \leq \epsilon \wedge d(x, x_n) \leq \epsilon$. A (quasi-)metric space is said to be (bi-)complete if every Cauchy sequence in the space has a (bi-)limit. A subspace of a (bi-)complete (quasi-)metric space is said to be closed if every Cauchy sequence in the subspace converges to an element of the subspace.

Theorem 2.1 (Banach's contraction principle) *Let $f \in X \rightarrow X$ be a contraction on a bi-complete quasi-metric space $\langle X, d\rangle$. Then f has a unique fixpoint, denoted by $fp(f)$.*

□

3 Extended and controsimmetric quasi-metrics

With the purpose of representing, in a more expressive way, our notion of approximation, we consider a definition of quasi-metric extended to the interval $[0, +\infty]$. Consequently we will adapt the definition of contractive function and enrich the standard notions with the definition of *controsimmetric* quasi-metric.

An extended (quasi-)metric on a set X is a mapping $d \in X \times X \rightarrow [0, +\infty]$ satisfying the usual axioms. It is necessary to extend in an obvious way the usual order on real numbers, so that for any x, extended element, we have $x \leq +\infty$.

Keeping the previous definition of contractive function and using the extended definition of quasi-metric, the uniqueness of the fixpoint stated by Banach's theorem is no longer provable. To obtain uniqueness it is necessary to enforce the notion of contractive function:

Theorem 3.1 (Banach II) *Let $f \in X \rightarrow X$ be a contraction on a be-complete quasi-metric space $\langle X, d\rangle$, such that there exists i such that $\forall x, y \in X \ . \ d(f^i(x), f^i(y)) < +\infty$. Then f has a unique fixpoint, denoted by $fp(f)$.* □

In the following of this paper we consider the above enforced version of contractive function. In defining an AI on quasi-metric spaces the now introduced notion of controsimmetric quasi-metric will be useful. A quasi-metric d on a set X is said to be *controsimmetric* if for every $x, y \in X$ such that $d(x, y) < +\infty$ and $d(y, x) < +\infty$ then $d(x, y) = d(y, x) = 0$.

Theorem 3.2 *Any controsimmetric quasi-metric space is bi-complete.* □

An isometric and surjective function between two quasi-metric spaces is said to be an *isomorfism* between them. It is easy to show that every isometric function is injective. Furthermore, if $\langle L_1, d_1\rangle$ is a quasi-metric space and $\langle L_2, d_2\rangle$ an isomorfic space, then $\langle L_2, d_2\rangle$ is a quasi-metric space, if $\langle L_1, d_1\rangle$ is bi-complete, so it is $\langle L_2, d_2\rangle$ and if $\langle L_1, d_1\rangle$ is controsimmetric, so it is $\langle L_2, d_2\rangle$.

4 Soundness of an AI on quasi-metric spaces

In AI the abstract semantics is proved to be sound with respect to a more concrete semantics. The concrete and abstract semantics of a program P, written in a language $\mathcal{L}$, are often solutions of fixpoint equations associated with P, of the type:

$$F_P(x) = x \quad \text{(concrete equation)} \qquad F_P^A(a) = a \quad \text{(abstract equation)}$$

Supposing to apply Banach's fixpoint theorem, we consider as concrete and abstract domains (of computation) the bi-complete quasi-metric spaces $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ respectively. The soundness proof of an analysis means to prove that $(fp(F_P), fp(F_P^A)) \in \psi$, where $\psi \subseteq (C \times A)$ is the soundness relation.

The following well known result is fundamental for proving the soundness Theorem 4.2 of an AI on quasi-metric spaces. This theorem corresponds to a similar one for the classical AI framework, where domains are usually structured as complete lattices (or CPOs) (see [8]).

Lemma 4.1 *Let $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ be bi-complete quasi-metric spaces and $d^\times$ such that $d^\times((c_1, a_1), (c_2, a_2)) = \max\{d_C(c_1, c_2), d_A(a_1, a_2)\}$. Then $\langle C \times A, d^\times\rangle$ is a bi-complete quasi-metric space* (see [1]). □

Theorem 4.2 *Let P be a program written in a language $\mathcal{L}$. Let $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ be any two bi-complete quasi-metric spaces and $\psi \subseteq (C \times A)$ be such that $\langle \psi, d^\times\rangle$ is a closed subspace of $\langle C \times A, d^\times\rangle$. Let F_P and F_P^A be two contractive mappings on $\langle C, d_C\rangle$ and on $\langle A, d_A\rangle$ respectively, such that $(c, a) \in \psi \Rightarrow (F_P(c), F_P^A(a)) \in \psi$. If ψ is a non empty relation, then $(fp(F_P), fp(F_P^A)) \in \psi$.* □

Theorem 4.3 *If $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ are controsimmetric quasi-metric spaces, so it is the quasi-metric space $\langle C \times A, d^\times\rangle$.* □

Observation 4.4 If d is controsimmetric, $\langle \psi, d^\times\rangle$ is always closed (Theorem 3.2). Thus considering controsimmetric spaces ensures an important hypothesis of Theorem 4.2 to hold.

5 Design of an AI on quasi-metric spaces

For any two elements $x, y \in \langle X, d\rangle$, we say that x is approximated by y if and only if $d(x, y) < +\infty$. Therefore the value of the distance d between two elements con be interpreted as the error introduced by the approximation: The lower is the value of the error $d(x, y)$, the better is the approximation. $d(x, y) = +\infty$ expresses naturally the fact that y does not approximate x.

In AI on quasi-metric spaces, it may be of peculiar importance to distinguish between the quasi-metric used in computation and that used in approximation; consequently it is possible to release the error representation from purely computation matters. This corresponds to separate the computation order from the approximation order, as stated by the classical framework of AI (e.g. strictness analysis, see [9]).

In the following, we define the notion of approximation space, which corresponds to a very general metric version of that of approximation set in classical AI. Actually the only hypothesis required is the existence of an approximating element for every element of the concrete domain. This is, on the other hand, a sufficient condition to ensure the existence of an AI.

Definition 5.1 *Let $\langle C, d_C \rangle$ be a quasi-metric space and $Y \subseteq C$. For any element $x \in C$, $H_Y(x) = \{y \in Y \mid d_C(x,y) < +\infty\}$ denotes the set of elements which approximate x and belong to Y. $\langle Y, d_C \rangle$ is an approximation space if $\forall x \in C \ . \ H_Y(x) \neq \emptyset$.*

In the classical framework of AI (see [6]), an approximation subspace can be defined by means of an operator, called approximation operator, on the concrete domain. In the following we define a notion of approximation operator on quasi-metric spaces.

Definition 5.2 *An operator ρ on a quasi-metric space $\langle C, d_C \rangle$ is an approximation operator if $\forall x \in C \ . \ d_C(x, \rho(x)) < +\infty$.*

Property 5.3 *If ρ is an approximation operator, then $\langle \rho(C), d_C \rangle$ is an approximation space.* □

We observe that, given an approximation space for a quasi-metric space, there exists always an approximation operator who generates it. Such operator may not be unique.

In order to represent an approximation space $\langle \rho(C), d_C \rangle$ in a computer memory we use an isomorfic quasi-metric space $\langle A, d_A \rangle$, named *representation space*. The isomorfism $\gamma \in A \rightarrow \rho(C)$ is the *concretization function*, while $\alpha = \gamma^{-1} \circ \rho$ is the *abstraction*. The following theorem shows that for the quasi-metric approximation it holds a property similar to the *only if* versus of adjunction, typical of the AI on posets.

Theorem 5.4 *Let $\langle C, d_C \rangle$ and $\langle A, d_A \rangle$ be any two quasi-metric spaces.*

(i) Let ρ be an approximation operator on $\langle C, d_C \rangle$ and $\langle A, d_A \rangle$ be a representation space for $\langle \rho(C), d_C \rangle$, with γ concretization function. If $\alpha = \gamma^{-1} \circ \rho$, then for all $c \in C$ and for all $a \in A$, $d_A(\alpha(c), a) < +\infty \Rightarrow d_C(c, \gamma(a)) < +\infty$ holds.

(ii) Let $\alpha \in C \rightarrow A$, $\gamma \in A \rightarrow C$ be any two mappings such that for all $c \in C$ and for all $a \in A$, $d_A(\alpha(c), a) < +\infty \Rightarrow d_C(c, \gamma(a)) < +\infty$ holds. Then $\gamma \circ \alpha$ is an approximation operator on $\langle C, d_C \rangle$.

□

5.1 Optimal approximation

In the following we try to further specify the notion of approximation, in order to ensure that, given an approximation space, there exists a unique approximation operator generating it.

Definition 5.5 *An approximation space $\langle M, d_C \rangle$ of $\langle C, d_C \rangle$ is an optimal approximation space if $\forall x \in C \ \exists y \in H_M(x) \ \forall u \in H_M(x) \ . \ d_C(x,y) \leq d_C(x,u)$. An approximation operator μ on $\langle C, d_C \rangle$ is an optimal approximation operator if $\forall x, u \in C \ . \ d_C(x, \mu(x)) \leq d_C(x, \mu(u))$.*

It is easy to verify that, if μ is an optimal approximation operator over $\langle C, d_C \rangle$, then $\langle \mu(C), d_C \rangle$ is an optimal approximation space. Furthermore if the regarded quasi-metrics satisfy a strengthened version of the *identity of indiscernibles*, then we can prove that:

Theorem 5.6 *Let $\langle C, d_C \rangle$ be a quasi-metric space such that for all $x, y \in C$ it holds $d_C(x,y) = 0 \Rightarrow x = y$. We can prove that:*

(i) Let $\langle M, d_C\rangle$ be an optimal approximation space, then the operator μ such that for all $x \in C$. $\mu(x) = m$, where m is such that $d_C(x,m) = \min_{z\in M}\{d_C(x,z)\}$, is the **unique** *best approximation operator for which $\mu(C) = M$ holds.*

(ii) If μ is an optimal approximation operator then it is idempotent, namely for all $x \in C$, $d_C(\mu(x), \mu(\mu(x))) = 0$ holds.

□

5.2 Connected approximation

The adjunction property, typical of classical AI, expresses the equivalence between two different soundness relations. Intuition wishes that soundness approximation of a concrete element c with an abstract element a happens indifferently when it can be stated that the abstraction of c is in approximation relation with a ($\alpha(c) \sqsubseteq a$), or the concretization of a approximates c ($c \sqsubseteq_C \gamma(a)$). We have seen that in the most general case of AI on quasi-metric spaces and also in the optimal approximation, this condition is not respected. In Theorem 5.4 actually holds '$\Rightarrow$' but not '$\Leftrightarrow$'. In the following we will try to strengthen the notion of approximation so that equivalence holds for quasi-metric based AI. We call *connected* those approximants of an element $c \in C$ whose distance from any other approximant of c is $< +\infty$.

Definition 5.7 *$\langle K, d_C\rangle$ approximation space of $\langle C, d_C\rangle$ is said to be a connected approximation space if $\forall x \in C\ \exists y \in H_K(x)\ \forall z \in H_K(x)$. $d_C(y,z) < +\infty$. An approximation operator κ on $\langle C, d_C\rangle$ is said to be a connected approximation operator if $\forall x \in C\ \forall z \in H_{\kappa(C)}(x)$. $d_C(\kappa(x), z) < +\infty$.*

Note that, if $\langle C, d_C\rangle$ is a **metric** space, then any approximation space $\langle Y, d_C\rangle$ is also a connected one. It is easy to verify that if κ is a connected approximation operator, then $\langle \kappa(C), d_C\rangle$ is a connected approximation space. Moreover we obtain the following results:

Theorem 5.8 *Let $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ be any two quasi-metric spaces.*

(i) Let ρ be a connected approximation operator on $\langle C, d_C\rangle$ and $\langle A, d_A\rangle$ a representation space for $\langle \rho(C), d_C\rangle$ with γ concretization function. If $\alpha = \gamma^{-1} \circ \rho$, then for all $c \in C$ and for all $a \in A$, $d_A(\alpha(c), a) < +\infty \Leftrightarrow d_C(c, \gamma(a)) < +\infty$ holds.

(ii) Let $\alpha \in C \to A$, $\gamma \in A \to C$ be any two functions such that for all $c \in C$ and for all $a \in A$, $d_A(\alpha(c), a) < +\infty \Leftrightarrow d_C(c, \gamma(a)) < +\infty$. Then $\gamma \circ \alpha$ is a connected approximation operator on $\langle C, d_C\rangle$ and $\alpha \circ \gamma$ is a connected approximation operator on $\langle A, d_A\rangle$.

□

Theorem 5.9 *Let $\langle C, d_C\rangle$ be a controsimmetric quasi-metric space.*

(i) Let $\langle K, d_C\rangle$ be a connected approximation space of $\langle C, d_C\rangle$. Then κ such that $\forall x \in C$. $\kappa(x) = u$, with u connected element in $H_K(x)$, is the **unique** *connected approximation operator satisfying $\kappa(C) = K$.*

(ii) If κ is a connected approximation operator, then it is idempotent, namely for all $x \in C$ $d_C(\kappa(x), \kappa(\kappa(x))) = d_C(\kappa(\kappa(x)), \kappa(x)) = 0$ holds.

□

5.3 Upper-closure approximation

In this section we try to redefine the notion of upper-closure operator adapting it to the case of quasi-metric spaces. As it can be seen a connected approximation can be obtained by means of such an operator. Hence it follows the interest in the connected approximation so as the natural quasi-metric counterpart of approximation in classical AI on posets.

Definition 5.10 *$\beta \in C \to C$ is an upper-closure operator on $\langle C, d_C \rangle$ if*

1. $\forall x \in C \,.\, d_C(x, \beta(x)) < +\infty$;
2. $\forall x \in C \,.\, d_C(\beta(x), \beta(\beta(x))) = 0$;
3. $\forall x, y \in C \,.\, d_C(x, y) < +\infty \Rightarrow d_C(\beta(x), \beta(y)) < +\infty$.

Theorem 5.11 *Let β be an upper-closure operator on $\langle C, d_C \rangle$. Then β is a connected approximation operator. Furthermore if the considered space is controsimmetric and β a connected approximation operator on it, then β is an upper-closure operator.* □

6 Soundness

In this section we study the soundness of an AI on quasi-metric spaces, as designed as shown in the previous section. Let ρ be an approximation operator on a concrete quasi-metric space $\langle C, d_C \rangle$ and γ concretization function (isomorfism) between the representation (abstract) space $\langle A, d_A \rangle$ and the approximation space. Also let $\alpha = \gamma^{-1} \circ \rho$ be the abstraction between concrete and abstract domain. We consider the following soundness relations:

$$(x, a) \in \psi \;\Leftrightarrow\; d_A(\alpha(x), a) < +\infty \tag{1}$$

$$(x, a) \in \psi' \;\Leftrightarrow\; d_C(x, \gamma(a)) < +\infty \tag{2}$$

Both relations satisfy the *existence of abstract approximations assumption* (see [8]) stating that:

$$\forall c \in C \; \exists a \in A \,.\, (c, a) \in \psi$$

It is clear that the relation ψ is stronger then ψ'. Actually for any kind of quasi-metric approximation, Theorem 5.4 holds; moreover in the connected approximation the two relations are equivalent (see Theorem 5.8).

In the following we distinguish between *approximation quasi-metrics* and *computation quasi-metrics*. With d_A and d_C we denote the approximation quasi-metrics on the concrete domain C and on the abstract domain A respectively; further we denote with d_{Cc} and d_{Ac} the computation quasi-metrics on C and A respectively. Let ψ be either the Relation (1) or (2) and choose the abstract function as $F_P^A = \alpha \circ F_P \circ \gamma$ which is, in the classical framework of AI, the best approximation for F_P in A (see [6]). The AI on quasi-metric spaces does not ensure that the approximation of the fixpoint semantics obtained with the function $\alpha \circ F_P \circ \gamma$ is the one with lowest error (distance) among all possible sound approximations. Actually even if an approximation is locally best, a locally worser choice may bring to a more precise final analysis. This fact is due to the triangle inequality of quasi-metrics.

For studying the soundness of an abstraction obtained with the framework above, we may apply Theorem 4.2. Therefore the following conditions have to be satisfied:

(a) $\langle C, d_{Cc}\rangle$ and $\langle A, d_{Ac}\rangle$ are bi-complete quasi-metric spaces;

(b) F_P and F_P^A are contractions on the respective quasi-metric computation spaces;

(c) if $(x, a) \in \psi$, then $(F_P(x), F_P^A(a)) \in \psi$.

The following theorems give sufficient conditions to satisfy the previous ones and so to prove the soundness of an analysis on quasi-metric spaces.

Theorem 6.1 *If $\langle C, d_{Cc}\rangle$ is bi-complete and $\langle \rho(C), d_{Cc}\rangle$ is a closed subspace, then $\langle A, d_{Ac}\rangle$ is bi-complete.* □

Theorem 6.2 *If F_P is a contraction, ρ a non expansive approximation operator and γ an isometric function on the respective quasi-metric computation spaces, then F_P^A is a contraction on $\langle A, d_{Ac}\rangle$.* □

Theorem 6.3 *Let ρ be an approximation operator and F_P any mapping on $\langle C, d_C\rangle$.*

(i) If $\forall x \in C\ \forall y \in \rho(C)\ .\ d_C(x, y) < +\infty \Rightarrow d_C(F_P(x), F_P(y)) < +\infty$ then (c) holds for the weak soundness Relation (2).

(ii) If $\forall x \in C\ \forall y \in \rho(C)\ .\ d_C(x, y) < +\infty \Rightarrow d_C(\rho \circ F_P(x), \rho \circ F_P(y)) < +\infty$ then (c) holds for the strong soundness Relation (1). □

When the quasi-metric of computation is the same as the one of approximation, as in most cases, then the following result holds:

Corollary 6.4 *Assume that the computation and approximation quasi-metrics be the same. Let the concrete space and the approximation subspace be respectively bi-complete and closed. If F_P is a contraction and ρ is non expansive on the concrete quasi-metric spaces, then $F_P^A = \alpha \circ F_P \circ \gamma$ brings to a sound AI with respect to the strong soundness Relation (1).* □

7 Examples

We consider two simple examples of application of abstract interpretation on quasi-metric spaces. For these examples we use logic programming (see [2]). Logic programming is an example of high-level language enjoying a simple semantic definition. Let B_P denote the Herbrand base for the language associated with a program P and T_P denote the usual immediate consequence operator associated with P.

7.1 Abstraction of non monotonic semantics

We consider the following logic program with negation P_e:

$$even(0) \leftarrow .$$
$$even(s(x)) \leftarrow \neg even(x).$$

It is well known that the immediate consequence operator T_e associated with P_e is not monotonic on $\langle \wp(B_e), \subseteq\rangle$ therefore Knaster-Trasky's fixpoint theorem is not applicable

to characterize the semantics of P_e. This fact prevents the applicability of classical AI, based on fixpoint approximation of monotonic functions. Fitting suggests Banach's fixpoint theorem as an alternative for defining the fixpoint semantics of P_e. This is obtained defining a proper complete metric space by means of a level mapping (see [12]): $\ell \in B_P \to \mathbb{N}$.

We consider, as level mapping for the previous program, the function ℓ_e such that $\ell_e(even(s^n(0))) = n$ and define a metric d_{ℓ_e} on $\wp(B_e)$ such that

$$d_{\ell_e}(I,J) = \begin{cases} 0 & \text{if } I = J \\ \frac{1}{n} & \text{if } I \text{ and } J \text{ differ on some ground atom of level } n > k \\ & \quad \text{but agree on all atoms of lower level} \\ +\infty & \text{otherwise} \end{cases}$$

where $k \in \mathbb{N}$ has been fixed, as we will see, according to the desired precision of analysis. Thus a metric space $\langle \wp(B_e), d_{\ell_e} \rangle$ is obtained, on which T_e is a contraction (see [12]).

Note that, with the previous metric we obtain a depth-k analysis. Actually a Herbrand interpretation I is approximated by an interpretation J (i.e. $d_{\ell_e}(I,J) < +\infty$) if they agree on all ground atoms of lower or equal level than k. In this case the operator $\rho_e(I) = \{q \in I \mid \ell_e(q) \leq k\}$ is an approximation operator that is both connected and optimal (see Section 5). The abstract properties describe the sets of natural numbers less or equal than k belonging to the respective Herbrand interpretations of P_e. Considering as equal the representation and the approximation spaces, as it often occurs in depth-k analysis (see [15]), the abstract operator $T_e^A = \lambda I \,.\, \rho_e \circ T_{e|\rho_e(\wp(B_e))}(I)$ ensures a sound analysis, namely Banach's fixpoint theorem and the Corollary 6.4 can be successfully applied. If $k = 3$ then the result of the analysis is $fp(T_e^A) = \{even(0), even(s^2(0))\}$ and $d_{\ell_e}(T_e, \gamma(T_e^A)) = \frac{1}{4}$ expresses the error introduced by the approximation. It is worth noting that by choosing a deeper level k, an analysis with lower error is obtained.

7.2 Error valuation

In the analysis of the following program P_6, we consider only the aspects of approximation through quasi-metrics.

$$p(0) \leftarrow .$$
$$p(s^6(x)) \longleftarrow p(x).$$

Because of the possibility of distinguishing between domains for computation and approximation, in this case we can consider the complete lattice $\langle \wp(B_6), \subseteq \rangle$ as domain for computation and a suitable quasi-metric for encoding the error in approximation. Therefore being T_6 monotonic on $\langle \wp(B_6), \subseteq \rangle$, Knaster-Tarsky's theorem can be used for characterizing fixpoint semantics, while the following quasi-metrics on Herbrand interpretations can be used to evaluate the error: $\ell_6(p(s^n(x))) = n$ is the level mapping and

$$d_{\ell_6}(I,J) = \begin{cases} 0 & \text{if } I = J \\ \frac{1}{2^n} & \text{if } I \subseteq J \text{ and differ on some ground atom of level } n \\ & \quad \text{and agree on all atoms of lower level} \\ +\infty & \text{otherwise} \end{cases}$$

Using d_{ℓ_6} it's possible, for example, to obtain a depth-k analysis, by choosing as approximation operator $\rho_6^k(I) = \{q \in I \mid \ell_6(q) \leq k\} \cup (B_6 \setminus B_{6|k})$, where the subset $B_{6|k} = \{q \in B_6 \mid \ell_6(q) \leq k\}$. The abstract semantics of P_6 is the least fixpoint of the usual

abstract function. Further, the error introduced by approximating the concrete semantics with this abstraction, is represented by the real value $d_{\ell_6}(lfp(T_6), lfp(T_6^{A_k})) = \frac{1}{2^{k+1}}$. It's worth noting that the deeper is the wished analysis (value k), the lower is the introduced error. In particular

$$\lim_{k \to +\infty} d_{\ell_6}(lfp(T_6), lfp(T_6^{A_k})) = 0$$

namely an exact approximation is obtained.

Instead a parity analysis can be obtained, by means of the following approximation operator:

$$\rho_6^p(I) = \begin{cases} I & \text{if } I = \emptyset \\ P & \text{if } I \subseteq P = \{p(s^{2i}) \mid i \in \mathbb{N}\} \cup \{p(0)\} \\ D & \text{if } I \subseteq D = \{p(s^{2i+1}) \mid i \in \mathbb{N}\} \\ B_6 & \text{otherwise} \end{cases}$$

The error introduced by the approximation in parity analysis is encoded by the quasi-metric d_{ℓ_6} and it is the real value $d_{\ell_6}(lfp(T_6), lfp(T_6^{A_p})) = \frac{1}{2}$.

Both analyses are comparable by the approximation error, while in the classical framework of AI they are not at all. Indeed with the previous quasi-metric, the error introduced by the parity analysis is greater than that introduced by the depth-k analysis. This because the quasi-metric d_{ℓ_6} considers only the measure of coincidence of abstract and concrete patterns, on the "initial" part (lowest level) only, while no weight is given to the coincidence at different, maybe regular, snapshots, as it might happen for example for parity analysis.

By choosing a different quasi-metric where more weight is given to regular sub expressions, it might happen that parity analysis becomes more precise then a depth-k analysis. This may happen for instance by choosing the following approximation quasi-metric, which is a variant of the Hausdorff quasi-distance (see [13]):

$$\bar{d}(I, J) = \begin{cases} 0 & \text{if } I = \emptyset \\ \sup_{y \in J} \inf_{x \in I} d'(x, y) & \text{if } I \subseteq J \\ +\infty & \text{otherwise} \end{cases}$$

with $d'(x, y) = |\ell_6(x) - \ell_6(y)|$. The error introduced by the depth-k analysis is the real value $\bar{d}(lfp(T_6), lfp(T_6^{A_k})) = 3$; while that introduced by the parity analysis is $\bar{d}(lfp(T_6), lfp(T_6^{A_p})) = 2$.

8 Quasi-metrics and order relations

In this section we try to find a relation between quasi-metrics and partial orders, both as tools for representing a given notion of approximation. With any quasi-metric on a set L it may be associated a pre-order relation and conversely with any pre-order relation on L it may be associated a set of pseudo-quasi-metrics, among whom at least one quasi-metric exists. In particular, the transfer from a quasi-metric to an order relation seems to be an approximation step. In that sense we would like to formalize it as an abstract interpretation, or rather by a Galois connection. Consequently a significant relation between classical AI and quasi-metric AI is given. Authors already dealt with the problem of establishing a correspondence between quasi-metric and pre-orders or partially ordered sets, e.g. [17, 19]. These approaches differ from our, which may have some analogies with that in [16].

Definition 8.1 *Let L be a set.*

- *A metric induced from the relation $\sqsubseteq$ on L is a mapping $d_{\sqsubseteq} \in (L \times L) \to \mathbb{R}^{0+}$ which satisfies reflexivity, triangle inequality and $\forall x, y \in L \,.\, d_{\sqsubseteq}(x,y) < +\infty \Leftrightarrow x \sqsubseteq y$.*
- *Let $d \in (L \times L) \to [0, +\infty]$ be a mapping. The relation induced from d on L is $\sqsubseteq_d \subseteq (L \times L)$ where for all $x, y \in L \,.\, x \sqsubseteq_d y \Leftrightarrow d(x,y) < +\infty$.*

Two quasi-metrics on a set I are said to be structural equivalent ($d_1 \overset{s}{\approx} d_2$) if they both induce the same relation, following the above definition, i. e. $\sqsubseteq_{d_1} = \sqsubseteq_{d_2}$.

Let $QM(I)$ denote the set of quasi-metrics on I and $QMc(I)$ be the set of all controsimmetric quasi-metrics on I. The situation may be resumed as following:

$$\begin{array}{ccccc} QM(I) & \twoheadrightarrow & QM_{|\overset{s}{\approx}}(I) & \longleftrightarrow & PRE(I) \\ \downarrow & & \downarrow & & \downarrow \\ QMc(I) & \twoheadrightarrow & QMc_{|\overset{s}{\approx}}(I) & \longleftrightarrow & PO(I) \end{array}$$

$\longleftrightarrow$ denotes a representation relation, i. e. an isomorfism, obtained by using Definition 8.1. By $\twoheadrightarrow$ or by $\longrightarrow$ we denote some approximation between sets: The approximation of type $\twoheadrightarrow$ consists in loosing the notion of error encoded by a distance, whereas only the notion of approximation is maintained. This is obtained by quotienting $QM(I)$ with respect to the relation of structural equivalence $\overset{s}{\approx}$ between quasi-metrics. The approximation of type $\longrightarrow$ consists in approximating a pre-order with a partial order (or equivalently a quasi-metric by a controsimmetric quasi-metric). The latter approximation step is the most hardly representable by a Galois connection, because the required adjunction has to consistently express the common notion of approximation expressed in quasi-metrics and pre-orders.

9 Conclusions

The main features of quasi-metric AI are the to express the error introduced by the approximation of semantics and the possibility of applying Banach's theorem to analyze non monotonic semantics, that cannot be analyzed with the classical framework for AI. The applicability in itself of Banach's theorem might seem to be a limit with respect to the applicability of Knaster-Tarsky's theorem, because Banach's ensures the existence of a unique fixpoint. Nevertheless note that a quasi-metric approach to AI is always possible, by encoding an order relation with an induced metric (see Definition 8.1). We believe that the major application fields of the presented theory are the study of approximated semantics for concurrency, where the approximation between processes can be conveniently defined by means of quasi-metrics (see [1, 3, 14, 17]). Moreover it might be interesting to combine the classical framework for AI with the AI on quasi-metric spaces, with the aim of applying numeric methods to the program analysis (e.g relative error, absolute error).

Acknowledgments. This paper was taken out of the Thesis [10]. Thanks to my advisor Roberto Giacobazzi.

References

[1] P. America and J. Rutten. Solving reflexive domain equations in a category of complete metric spaces. *Journal of Computer and System Sciences*, 39(3):343–375, 1989.

[2] K. R. Apt. Logic programming. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Models and Semantics, pages 495–574. Elsevier and The MIT Press, Amsterdam and Cambridge Mass., 1990.

[3] J. W. Bakker and J. I. Zucker. Processes and the denotational semantics of concurrency. *Information and Control*, 54(1-2):70–120, 1982.

[4] P. Cousot. Abstract interpretation. *ACM Computing Surveys*, 28(2):324–328, 1996.

[5] P. Cousot and R. Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the 4th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977.

[6] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Conference Record of the 6th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 269–282, San Antonio, Texas, 1979.

[7] P. Cousot and R. Cousot. Abstract interpretation and application to logic programs. *Journal of Logic Programming*, 13(2-3):103–179, 1992.

[8] P. Cousot and R. Cousot. Abstract interpretation frameworks. *Journal of Logic and Computation*, 2(4):511–547, 1992.

[9] P. Cousot and R. Cousot. Higher-order abstract interpretation (and application to comportment anaysis generalizing strictness, termination, projection an PER analysis of functional languages). In *Proceedings of the 1994 International Conference on Computer Languages*, pages 95–112. IEEE Computer Society Press, 1994.

[10] F. Crazzolara. Spazi quasi-metrici come domini per l'interpretazione astratta e l'analisi di programmi. Master's thesis, University of Pisa, february 1997. Advisor R. Giacobazzi.

[11] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.

[12] M. Fitting. Metric methods: Three examples and a theorem. *Journal of Logic Programming*, 21(3):113–127, 1994.

[13] F. Hausdorff. *Mengenlehre*. Walter de Gruyter & Co., Leipzig, 1929.

[14] M. E. Majster-Cederbaum and F. Zetzsche. Towards a foundation for semantics in complete metric spaces. *Information and Computation*, 99:217–243, 1991.

[15] K. Marriott and H. Søndergaard. Bottom-up dataflow analysis of normal logic programs. *Journal of Logic Programming*, 13(2-3):181–204, 1992.

[16] Rowlands-Hughes. *Domains versus metric spaces*. Master's thesis, Department of Computing, Imperial College, 1987.

[17] J. J. M. M. Rutten. Elements of generalized ultrametric domain theory. *Theoretical Computer Science*, 170:349–381, 1996.

[18] A. K. Seda. Quasi-metrics and the semantics of logic programs. *Bulletin of the European Association for Theoretical Computer Science*, 60:154–163, 1996.

[19] M. B. Smyth. Quasi-uniformities: Reconciling domains with metric spaces. In *Proceedings of the 3rd Workshop on Mathematical Foundations of Programming Language Semantics*, volume 298 of *Lecture Notes in Computer Sciences*, pages 236–253, Berlin, 1987. Springer-Verlag.

[20] M. B. Smyth. Topology. In *Handbook of Logic in Computer Science*, volume 1, pages 641–761. Oxford University Press, 1992.

[21] W. A. Wilson. On quasi-metric spaces. *Amer. J. Math.*, 53:675–684, 1931.