NUI MAYNOOTH
Ollscoil na hÉireann Má Nuad

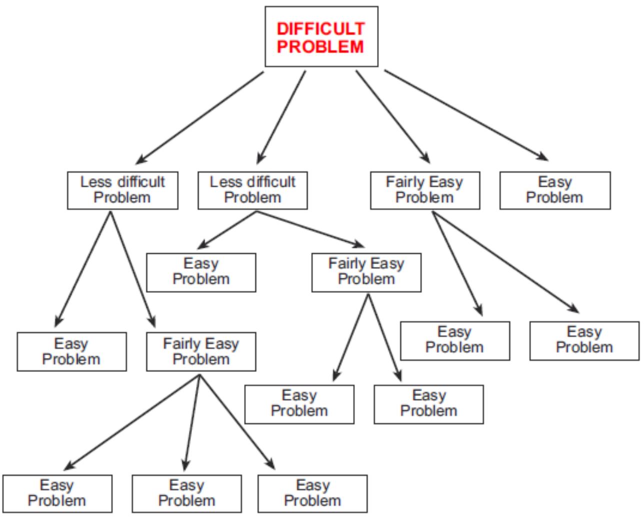
IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

REFINEMENT – BACK

Overview

Introduction

- Refinement calculus is a framework for reasoning about correctness and refinement of programs.
- Stepwise refinement



Predicate Transformers

- Refinement calculus is an extension of Dijkstra’s weakest precondition calculus where program statements are modelled as predicate transformers.
- Definition is extended to contracts that regulate the behaviour of competing agents and to two-player games.

Agents

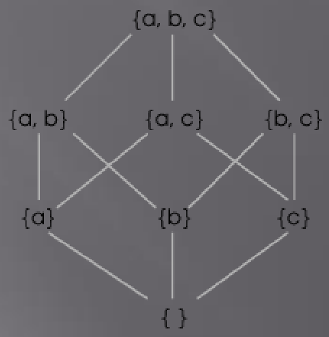
- An agent has the ability to change the world in various ways through actions that it can choose between.
- The behaviour of these agents is regulated by contracts.

Contracts as games

- A player in a game has a "winning strategy" in a certain initial state if the player can win no matter what the opponent does.
- Satisfaction of a contract corresponds to having a winning strategy:
  - $\sigma\{|S|\}q$ holds iff our agent has a winning strategy to reach the goal q, when playing with rules S starting in initial state σ.
- If our agent is forced to breach an assertion then it loses the game. If the other agent is forced to breach an assertion then it loses and our agent wins.

Posets

- A relation ⊑ is called a preorder if it is reflexive and transitive.
- The pair (A, ⊑) is then called a “preset”
- If the preorder is also anti symmetric it is said to be a partial order and (A, ⊑) is a “poset”.



Lattices

- A poset (A, $\sqsubseteq$) is called a lattice if the meet $a \sqcap b$ and join $a \sqcup b$ exist in A for all pairs a, b of elements of A.
  - A poset is a lattice iff $\sqcap B$ and $\sqcup B$ exist for all finite nonempty subsets B of A.

Lattice Algebra

1. $a \sqcap a = a \quad a \sqcup a = a$ (idempotence)
2. $a \sqcap b = b \sqcap a \qquad a \sqcup b = b \sqcup a$ (commutativity)
3. $a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c \quad a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$ (associativity)
4. $a \sqcap (a \sqcup b) = a \qquad a \sqcup (a \sqcap b) = a$ (absorption)
5. Meet and join are monotonic with respect to lattice ordering

Tarski Consequence Axioms:

☑ Axiom 3: If $X \subseteq S\ then\ Cn\big(Cn(X)\big) = Cn(X)$ (idempotence)

☑ Axiom 4: If $X \subseteq S\ then\ Cn(X) = \sum_{Y \subseteq X\ and\ |Y| < \aleph_0} Cn(Y)$ (compactness => monotonicity)

Abstract Categories

- A category C consists of a collection of objects Obj(C) and a collection of morphisms Mor(C)

$$\begin{tikzcd} \underset{\text{Source}}{A} \arrow[r, "f"] & \underset{\text{Target}}{B} \end{tikzcd}$$

- The analogue to lattice homomorphism in a category is a functor. Given to categories C and D, functor F maps objects of C to objects of D and morphisms of C to morphisms of D.

Refinement

- Refinement is defined as a relationship between contracts and is a lattice ordering
- Correctness is a special case of refinement where a specification is refined by a program.

Refinement Calculus

- All the basic domains of the refinement calculus are order-enriched categories, in most cases different kinds of lattice-enriched categories.
- The refinement calculus is a single collection of inference rules based on the general lattice and categorical properties of order-enriched categories

ANY
QUESTIONS
?