Metric Coinduction

Problems for Solution

May 8, 2009

Please solve problems 1, 2, and either 3 or 4. Some useful definitions are given at the end. Please use LaTeX and and submit a `.pdf` file by June 15, 2009 to `kowalik AT mimuw DOT edu DOT pl`. Please include your name and email address.

1. (Easy) Let M be a complete metric space and $\tau : M \to M$ a contractive map. Recall that the *metric coinduction principle* says: If φ is a nonempty closed subset of M preserved by τ, then the unique fixpoint of τ is in φ. Prove the validity of this principle. You may assume the *Banach fixpoint theorem* without proof: Every contractive map on a complete metric space has a unique fixpoint.

2. (Medium) Consider the following protocol for simulating a bias-q coin with a bias-p coin for $0 < p < 1/2$, $0 \le q \le 1$. In each step, we flip the p-coin, which returns heads with probability p and tails with probability $1 - p$. (This is one of the protocols we discussed in the lecture on Monday.)

   (i) If $q \le p$ and the outcome of the p-coin flip was tails, halt and declare tails for the q-coin.

   (ii) If $q \le p$ and the outcome of the p-coin flip was heads, rescale the problem, setting $q := q/p$, and repeat.

   (iii) If $q \ge 1-p$ and the outcome of the p-coin flip was tails, halt and declare heads for the q-coin.

   (iv) If $q \ge 1 - p$ and the outcome of the p-coin flip was heads, rescale the problem, setting $q := (q - (1 - p))/p$, and repeat.

   (v) If $p < q < 1 - p$ and the outcome of the p-coin flip was heads, halt and declare heads for the q-coin.

   (vi) If $p < q < 1 - p$ and the outcome of the p-coin flip was tails, rescale the problem, setting $q := (q - p)/(1 - p)$, and repeat.

   Let $E(q)$ be the expected running time of the protocol on q. Prove coinductively that for all q in the interval $p < q < 1 - p$, $E(q) \ge 2$ (*Hint.* You may have to strengthen the coinduction hypothesis slightly!) and that $E(p) = E(1 - p) = 1/(1 - p) < 2$. Thus E is discontinuous at p and $1 - p$.

3. (Difficult) For any function $f : A \to B$, let $\mathsf{map}\, f : \mathsf{Stream}\, A \to \mathsf{Stream}\, B$ be the function that applies f to all elements of its input stream. For example, if s is the successor function on $\mathbb{Z}$, then $\mathsf{map}\, s\ (57, 12, -392, \ldots) = (58, 13, -391, \ldots)$. Give a formal coinductive definition of $\mathsf{map}\, f$ in terms of head and tail; do not use the informal notation with ellipsis $(\ldots)$ as above or the list constructor $::$. Argue that $\mathsf{map}\, f$ is uniquely defined. Prove coinductively that if $f : A \to B$ and $g : B \to A$ are inverses, then so are $\mathsf{map}\, f$ and $\mathsf{map}\, g$.

4. (Difficult) Define the functions

$$\mathsf{fib} : \mathbb{Z}^2 \to \mathsf{Stream}\, \mathbb{Z} \qquad\qquad \mathsf{add} : (\mathsf{Stream}\, \mathbb{Z})^2 \to \mathsf{Stream}\, \mathbb{Z}$$

coinductively as follows:

$$\begin{aligned} \mathsf{head}(\mathsf{fib}(n,m)) &= n & \mathsf{head}(\mathsf{add}(\sigma,\tau)) &= \mathsf{head}(\sigma) + \mathsf{head}(\tau) \\ \mathsf{tail}(\mathsf{fib}(n,m)) &= \mathsf{fib}(m, n+m) & \mathsf{tail}(\mathsf{add}(\sigma,\tau)) &= \mathsf{add}(\mathsf{tail}(\sigma), \mathsf{tail}(\tau)). \end{aligned}$$

What is $\mathsf{fib}(1,1)$? Argue that fib and add are uniquely defined. Prove coinductively that

$$\mathsf{add}(\mathsf{fib}(n,m), \mathsf{tail}(\mathsf{fib}(n,m))) \quad = \quad \mathsf{tail}(\mathsf{tail}(\mathsf{fib}(n,m))).$$

5. (Open problem) Consider the protocol of Question 2. Instead of clauses (v) and (vi), we might have used

   (v′) If $p < q < 1 - p$ and the outcome of the p-coin flip was heads, halt and declare tails for the q-coin.

   (vi′) If $p < q < 1 - p$ and the outcome of the p-coin flip was tails, rescale the problem, setting $q := q/(1-p)$, and repeat.

   In fact, whenever $p < q < 1 - p$, we can choose to follow either (v) and (vi) or (v′) and (vi′). The choice may depend on q. We would like to choose the option that minimizes the expected running time. For given rational p and q, is this decidable?

(See the next page for definitions)

Useful Definitions

- A *metric space* M is a set with a *distance function* $d : M \times M \to \mathbb{R}$ such that
  - $d(x, y) \geq 0$, and $d(x, y) = 0$ iff $x = y$
  - $d(x, y) = d(y, x)$ (symmetry)
  - $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality)
- A metric space (M, d) is *complete* if every Cauchy sequence converges to a point in M.
- A sequence $x_0, x_1, \ldots$ in M is *Cauchy* if for all real $\varepsilon > 0$ there exists an integer $N \geq 0$ such that for all $m, n \geq N$, $d(x_m, x_n) < \varepsilon$.
- A sequence $x_0, x_1, \ldots$ *converges* to x if for all real $\varepsilon > 0$, there exists an integer $N \geq 0$ such that for all $n \geq N$, $d(x, x_n) < \varepsilon$.
- A set $A \subseteq M$ is *closed* if it contains all its limit points.
- A *limit point* of a set $A \subseteq M$ is an element $x \in M$ such that for all real $\varepsilon > 0$, there exists $y \in A$ such that $d(x, y) < \varepsilon$.
- A function $\tau : M \to M$ is *contractive* if there exists a real number $c < 1$ such that for all $x, y \in M$, $d(\tau(x), \tau(y)) \leq c \cdot d(x, y)$.
- A set $A \subseteq M$ is *preserved by* $\tau : M \to M$ if for every $x \in A$, $\tau(x) \in A$.
- A point $x \in M$ is *fixpoint* of $\tau : M \to M$ if $\tau(x) = x$.
- The structure $\mathsf{Stream}\, A = (A^\omega, \mathsf{head}, \mathsf{tail})$ is the coalgebra of infinite streams over the set A with operations

  $$\mathsf{head} : \mathsf{Stream}\, A \to A \qquad \mathsf{tail} : \mathsf{Stream}\, A \to \mathsf{Stream}\, A.$$

  It is the final coalgebra in the category of simple transition systems with observations A.
- A *simple transition system with observations* A is a structure $(X, \mathsf{obs}, \mathsf{cont})$ consisting of a set X and operations

  $$\mathsf{obs} : X \to A \qquad \mathsf{cont} : X \to X.$$

- A *homomorphism* from $(X, \mathsf{obs}_X, \mathsf{cont}_X)$ to $(Y, \mathsf{obs}_Y, \mathsf{cont}_Y)$ is a function $h : X \to Y$ such that for all $x \in X$,

  $$\mathsf{obs}_Y(h(x)) = \mathsf{obs}_X(x) \qquad \mathsf{cont}_Y(h(x)) = h(\mathsf{cont}_X(x)).$$

- A coalgebra C is *final* (or *terminal*) in a category of coalgebras if there is a unique homomorphism from every coalgebra in the category to C.