GLOBAN Assignment:
Advanced Solver Technology

1. Design a non-trivial program analysis which computes for every predicate p/k defined by a given set S of Horn clauses, a set of argument positions $[p/k]^\sharp \subseteq \{1, \ldots, k\}$ which definitely hold only finitely many terms in the least model of S.

   (a) Evaluate your Analysis on the following set of clauses:

$$\begin{array}{lcl} p(X,Y) & \Leftarrow & q(a(Y), b(X,Y)) \\ q(a(X),Y) & \Leftarrow & q(X,Y) \\ q(c, b(c,c)) & \Leftarrow & \end{array}$$

It should return:

$$[p/2]^\sharp = \{1, 2\} \qquad\qquad [q/2]^\sharp = \{2\}$$

(b) Argue that your analysis is correct!

(c) Is your analysis also able to detect finiteness of the second argument of $p/2$ if there were a clause:

$$p(X, a(Y)) \quad \Leftarrow \quad q(a(Y), b(X, Y))$$

If not: what can be done about it?

2. Search the Web for a non-trivial cryptographic protocol different from the Needham-Schroeder protocol.

   Assume that all messages are sent through in-secure channels. Characterize the knowledge of an attacker by means of Horn clauses.

   In which sense is your formalization correct?

   Check whether an attacker might get hold of the secret by means of the fh1 solver!