CS 476 Homework #7 Due 10:45am on 3/24

Note: Answers to the exercises listed below as well as the Maude code for Exercise 2 should be emailed to `abir2@illinois.edu` in *typewritten form* (latex formatting preferred) by the deadline mentioned above.

1. Solve Exercise 100 in *STACS*.

   Note. Your equality proofs should *only use the axioms of the theory of groups listed in Exercise 100* in *STACS* and no other equations. However, equations already proved using such axioms can also be used as *lemmas* to prove other equations.

2. Consider the following functional theory specifying an alternative axiomatization of the *theory of groups*, where `i` denotes the *inverse* operation $(\_)^{-1}$

```
set include BOOL off .

fth GROUP is
  sort Group .
  op 1 : -> Group .
  op i : Group -> Group .
  op _*_ : Group Group -> Group .

  var x y z : Group .
  eq  (x * y) * z    = x * (y * z) .
  eq  1 * x          = x .
  eq  x * 1          = x .
  eq  x * i(x)       = 1 .
  eq  i(x) * x       = 1 .
  eq  i(1)           = 1 .
  eq  i(i(x))        = x .
  eq  i(x * y)       = i(y) * i(x) .
  eq  x * (i(x) * y) = y .
  eq  i(x) * (x * y) = y .
endfth
```

   Do the following:

   (a) Prove that the module `GROUP` is locally confluent by using the Church-Rosser Checker tool.

   (b) Use the MTA tool to prove the termination of `GROUP`.
   Hint. This module has a termination poof by an $A \vee C$-RPO order.

   (c) What can you now conclude from (a) and (b) above about *provable equality* in the theory of groups using *this* axiomatization of the theory of groups instead of the axiomatization in Exercise 100 in *STACS*? Specifically, giving any equation $u = v$ in the signature of `GROUP`, can one *decide*, i.e., effectively and mechanically give a yes/no answer, to the question of wether $u = v$ can be *proved* using the equations of the theory of groups, and if so, how? Justify your answer.

   (d) (For 8 points of *extra credit*, i.e., you could get as much as 18 points instead of the usual 10 for Exercise 2 if you did everything right, including this extra part). Call two equational theories (Σ, E) and (Σ, E') *equivalent* (denoted $(\Sigma, E) \equiv (\Sigma, E')$) iff: (i) $\forall(u' = v') \in E', \quad (\Sigma, E) \vdash u' = v'$, and (ii) $\forall(u = v) \in$

$E,\ \ (\Sigma, E') \vdash u = v$. Prove in detail that the theory of groups in Exercise 100 in *STACS* and the confluent and termination axiomatization in `GROUP` above are equivalent theories in this precise sense. **Important Remark**. Note that Exercise 2 would be nonsense in case the two formulation of the theory of groups you are comparing were not equivalent in the precise sense just defined.