IA085: Satisfiability and Automated Reasoning

Seminar 6

Exercise 1 *For each of the following first-order entailments, decide whether it holds or not. If it does not hold, provide a counterexample. If it does, prove it by resolution.*

1. $\forall x.\, P(x) \models \neg\exists x.\, \neg P(x)$
2. $\forall x \exists y.\, S(x,y) \models \exists y \forall x.\, S(x,y)$
3. $(\forall x \exists y.\, S(x,y)) \wedge (\forall x \forall y.\, P(x) \wedge S(x,y) \rightarrow P(y)) \wedge P(a) \models \forall x.\, P(x)$
4. $(\forall x \forall y.\, S(x,y)) \wedge (\forall x \forall y.\, P(x) \wedge S(x,y) \rightarrow P(y)) \wedge P(a) \models \forall x.\, P(x)$

Exercise 2 *For each of the following first-order entailments with interpreted equality, decide whether it holds or not. If it does not hold, provide a counterexample. If it does, prove it by superposition calculus.*

1. $\exists x \forall y.\, f(y) = x \;\models\; \forall x \forall y.\, g(f(x)) = g(f(y))$
2. $\forall x \forall y.\, R(x,y) \rightarrow f(x) = y \;\models\; \forall x \forall y \forall z.\, R(x,y) \wedge R(x,z) \rightarrow y = z$
3. $(\forall x.\, f(g(x)) = x) \wedge (\forall x.\, g(f(x)) = x) \;\models\; \forall x \exists y.\, x = f(y)$
4. $\forall x \forall y.\, (P(y) \wedge y = f(x)) \rightarrow P(x) \;\models\; \forall x.\, P(f(f(x))) \rightarrow P(x)$

Exercise 3 *Download the automated theorem prover Vampire and try proving the following theorem, written in the* TPTP *language. What does the theorem say?*

`https://tptp.org/UserDocs/TPTPLanguage/TPTPLanguage.shtml`

```
fof(ass, axiom, ! [X,Y,Z] : mult(mult(X,Y),Z) = mult(X,mult(Y,Z))).
fof(li,  axiom, ! [X] : mult(e,X) = X).
fof(ri,  axiom, ! [X] : mult(X,e) = X).

fof(unq, conjecture, ! [E2] : (! [X] : mult(X,E2) = X & mult(E2,X) = X) => e = E2).
```

Exercise 4 *Use the theorem prover Vampire to prove some of the entailments from Exercises 1 and 2.*

Exercise 5 *Use the theorem prover Vampire to prove the following theorem:*

- *Let R be a commutative ring. If R has characteristic three (i.e. $1+1+1=0$), R includes the field $\mathbb{F}_3$ with three elements.*