Logic and Proof

Supervision 3

9. Decision procedures and SMT solvers

1. In Fourier–Motzkin variable elimination, any variable not bounded both above and below is deleted from the problem. For example, given the set of constraints

$$3x \geq y \qquad x \geq 0 \qquad y \geq z \qquad z \leq 1 \qquad z \geq 0$$

   the variables x and then y can be removed (with their constraints), reducing the problem to $z \leq 1 \wedge z \geq 0$. Explain how this happens and why it is correct.

2. Apply Fourier–Motzkin variable elimination to the following sets of constraints.

   a) ① $x \geq z$ ② $y \geq 2z$ ③ $z \geq 0$ ④ $x + y \leq z$

   b) ① $x \leq 2y$ ② $x \leq y + 3$ ③ $z \leq x$ ④ $0 \leq z$ ⑤ $y \leq 4x$

3. Summarise the main ideas behind SMT solvers: how do they combine decision procedures with clause-based methods and what kinds of problems do they allow us to solve?

4. Apply the SMT algorithm sketched in the notes to the following set of clauses. Recall that the constraints $\boxed{c > 0}$ and $\boxed{c < 0}$ are unrelated.

$$\{c = 0, c > 0\} \qquad \{a \neq b\} \qquad \{c < 0, a = b\}$$

10. Binary decision diagrams

1. Compute the BDD for each of the following formulas, taking the variables as alphabetically ordered.

$$P \wedge Q \to Q \wedge P \qquad P \vee Q \to P \wedge Q \qquad \neg(P \vee Q) \vee P \qquad \neg(P \wedge Q) \leftrightarrow (P \vee R)$$

2. Verify these equivalences using BDDs.

$$(P \wedge Q) \wedge R \simeq P \wedge (Q \wedge R) \qquad (P \vee Q) \vee R \simeq P \vee (Q \vee R)$$
$$P \vee (Q \wedge R) \simeq (P \vee Q) \wedge (P \vee R) \qquad P \wedge (Q \vee R) \simeq (P \wedge Q) \vee (P \wedge R)$$
$$\neg(P \wedge Q) \simeq \neg P \vee \neg Q \qquad (P \leftrightarrow Q) \leftrightarrow R \simeq P \leftrightarrow (Q \leftrightarrow R)$$
$$(P \vee Q) \to R \simeq (P \to R) \wedge (Q \to R) \qquad (P \wedge Q) \to R \simeq P \to (Q \to R)$$

11. Modal logics

1. Explain why adding the T, 4 and B axioms make the transition relation reflexive, transitive and symmetric, respectively? Consider both the informal meaning and the formal semantics.

2. Why does the dual of an operator string equivalence also hold? For example, how can we deduce $\Diamond\Diamond A \simeq \Diamond A$ from $\Box\Box A \simeq \Box A$?

3. a) Prove the sequents $\Diamond(A \lor B) \Rightarrow \Diamond A, \Diamond B$ and $\Diamond A \lor \Diamond B \Rightarrow \Diamond(A \lor B)$, thus proving the equivalence $\Diamond(A \lor B) \simeq \Diamond A \lor \Diamond B$.

   b) Similarly, prove the equivalence $\Box(A \land B) \simeq \Box A \land \Box B$.

4. Prove the following sequents.

$$\Diamond(A \to B), \Box A \Rightarrow \Diamond B \qquad \Box\Diamond\Box A, \Box\Diamond\Box B \Rightarrow \Box\Diamond\Box(A \land B)$$

12. Tableaux-based methods

1. Use the free-variable tableau calculus to prove the following formulas.

$$(\exists y.\, \forall x.\, R(x,y)) \to (\forall x.\, \exists y.\, R(x,y))$$
$$(P(a,b) \lor \exists z.\, P(z,z)) \to \exists x,y.\, P(x,y)$$
$$((\exists x.\, P(x)) \to Q) \to (\forall x.\, P(x) \to Q)$$

2. Compare the sequent calculus, resolution and the free-variable tableau calculus by using each of them to prove the following formula.

$$(P(a,b) \lor \exists z.\, P(z,z)) \to \exists x,y.\, P(x,y)$$

Optional exercise

Temporal logic is not the only type of modal logic: depending on how we interpret $\Box A$, we can admit different axioms and relational properties for our logic. Some are of philosophical interest, while others have found use in computer science and mathematics. Below are a few examples:

Name	**Domain**	**Interpretation of $\Box A$**	**Interpretation of $\Diamond A$**
Temporal	time	A always holds	
Alethic	necessity		A possibly holds
Doxastic	belief	I believe that A holds	
Epistemic	knowledge		For all I know, A holds
Deontic	duty	It is obligatory that A holds	

a) Complete the table either by intuition or through research. Recall that $\Diamond A$ is defined as $\neg\Box\neg A$.

b) Assign each of the formulae below to the modal logics in which they could be reasonably assumed as axioms. For example, does belief of A imply the truth of A?

   a) $\Box(A \to B) \land \Box A \to \Box B$
   b) $\Box A \to A$
   c) $\Box A \to \Box\Box A$
   d) $\Diamond A \to \Box\Diamond A$
   e) $\Diamond\top$
   f) $\Box A \to \Diamond A$

c) *Provability logic* is an interesting variant of a modal logic which interprets $\Box A$ as "A *is provable in the theory* T" where T is some axiomatic system that we are working in (such as Peano arithmetic). What (if anything) can we say about a particular system T if we know that:

(i) the formula $\Box A \to A$ is an axiom?

(ii) the formula $\neg\Box\bot$ is an axiom?

(iii) the formula $\Box A \to \Diamond A$ is *not* an axiom?