Logic and Proof

Supervision 3 – Solutions

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 $z \leq 1 \land z \geq 0$. Explain how this happens and why it is correct.

   > If a variable w is constrained in only one direction, then a suitable value for it can be calculated after the constraints on the other variables have been solved. If the set of constraints is ultimately unsatisfiable, this will never be due to the variable not constrained on both sides since unsatisfiable constraints must be reducible to $w \leq l$ and $u \leq w$ for some $l < u$. In the example above, x starts with having no upper bounds, so its value can be selected to be an arbitrarily large value once the constraints for other variables have been satisfied. Removing the first two terms also leaves y without any upper bounds, so it too can be eliminated. The remaining constraints involving z are easily satisfied as $z = 0$ or $z = 1$, and values for y, then x can be chosen accordingly afterwards; for instance, $y = 1$ and $x = 3$.

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 $x + y \leq z$

   > Eliminate x by combining ① $z \leq x$ and ④ $x + y \leq z \longleftrightarrow x \leq z - y$ to get $z \leq z - y$, which is equivalent to ⑤ $y \leq 0$.
   >
   > ② $y \geq 2z$ ③ $z \geq 0$ ⑤ $y \leq 0$
   >
   > Eliminate y by combining ② $2z \leq y$ and ⑤ $y \leq 0$ to get $2z \leq 0$, i.e. ⑥ $z \leq 0$.
   >
   > ③ $z \geq 0$ ⑥ $z \leq 0$
   >
   > This is satisfiable with $z = 0$; the previous constraint $2z \leq y \leq 0$ implies $y = 0$ and $z \leq x \leq z - y$ implies $x = 0$.

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

   > Eliminate z by combining ④ $0 \leq z$ and ③ $z \leq x$ to get ⑥ $0 \leq x$.
   >
   > ① $x \leq 2y$ ② $x \leq y + 3$ ⑤ $\dfrac{y}{4} \leq x$ ⑥ $0 \leq x$
   >
   > Eliminate x by combining: ⑥ and ① to get $0 \leq 2y \longleftrightarrow 0 \leq y$; ⑥ and ② to get

> $0 \leq y+3 \leftrightarrow -3 \leq y$; ⑤ and ① to get $\frac{y}{4} \leq 2y \leftrightarrow 0 \leq y$ and ⑤ and ② to get $\frac{y}{4} \leq y+3 \leftrightarrow -4 \leq y$. In the resulting constraints y is only bounded from below so they are satisfiable; the most limiting constraint is $0 \leq y$. Again, a possible model is $x = y = z = 0$.

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?

> SMT solvers allow us to solve complex decision problems by separating purely logical reasoning from theory-specific constraints. An SMT instance is a FOL formula where the constant, function, and relation symbols have extrinsic interpretations, e.g. in the theory of real numbers and inequalities, lists or arrays, bit vectors, etc. While it may be possible to solve formulae purely symbolically (e.g. using first-order resolution), particular theories often have specialised decision procedures that are more efficient. If a formula is unsatisfiable, it may be due to some theory-specific conflict like $x \leq 0 \land 3 \leq x$, but it could be a purely logical contradiction like $x = 1 \land \neg(x = 1)$. SMT solvers turn the formula into clausal form, treating atomic formulae like $\boxed{x = 0}$ and $\boxed{y \leq 5}$ as opaque propositional letters, with the exception of some negated or dual relationships, such as interpreting $y \neq 1$ as $\neg\boxed{y = 1}$. In the first pass, a propositional model-finding algorithm like DPLL is used to “estimate” a model and weed out formulae which are logically inconsistent. The estimate – which may be vastly simpler than the original formula – is then passed on to the theory-specific decision procedure to confirm if it is indeed a model. If it is not, the decision procedure returns a refutation or counterexample to DPLL which can now refine its guess or conclude that no models it can propose are actually valid. This separation of responsibilities makes SMT solvers well suited for even very large formulas that occur in practical settings like system verification and automated theorem proving.

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.

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

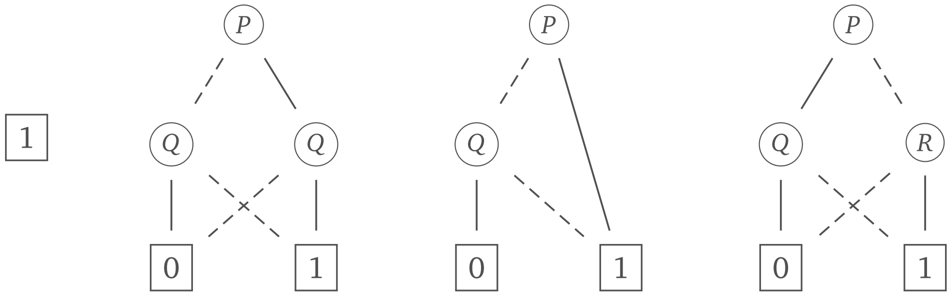
> The DPLL algorithm receives the following set of clauses of opaque literals:
>
> $$① \left\{\boxed{c = 0}, \boxed{c > 0}\right\} \qquad ② \left\{\neg\boxed{a = b}\right\} \qquad ③ \left\{\boxed{c < 0}, \boxed{a = b}\right\}$$
>
> Unit propagation removes clause ② and $\boxed{a = b}$ from clause ③.
>
> $$① \left\{\boxed{c = 0}, \boxed{c > 0}\right\} \qquad ③ \left\{\boxed{c < 0}\right\}$$
>
> Again, we unit propagate ③ which doesn’t affect ①.
>
> $$① \left\{\boxed{c = 0}, \boxed{c > 0}\right\}$$
>
> Now, we choose a literal to do a case split on; if $\boxed{c = 0}$ is true, ① is satisfied and we have

> the proposed DPLL model
>
> $$\boxed{a = b} \qquad \boxed{c < 0} \qquad \boxed{c = 0}$$
>
> which gets passed on to a decision procedure for inequalities. Analysing the contents of the literals, it is easy to see that the constraints are unsatisfiable, so the decision procedure returns the negation of the model which becomes an additional clause:
>
> $$④\ \left\{\neg\boxed{a = b}, \neg\boxed{c < 0}, \neg\boxed{c = 0}\right\}$$
>
> With the first case rejected, DPLL analyses the case $\neg\boxed{c = 0}$. Clause ④ gets deleted, and clause ① becomes ① $\left\{\boxed{c > 0}\right\}$, which, upon unit propagation, gives another model
>
> $$\boxed{a = b} \qquad \boxed{c < 0} \qquad \neg\boxed{c = 0} \qquad \boxed{c > 0}$$
>
> However, this too gets rejected by the decision procedure. Since no more backtracking is possible, the SMT solver concludes that the set of clauses is unsatisfiable.

10. Binary decision diagrams

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

$$P \land Q \to Q \land P \qquad P \lor Q \to P \land Q \qquad \neg(P \lor Q) \lor P \qquad \neg(P \land Q) \leftrightarrow (P \lor R)$$

> 
>
>
> The first formula is a tautology, so its canonical BDD is simply $\boxed{1}$ – upon construction we see that the case analyses on the individual propositions do not actually branch into distinct subdiagrams and can therefore be collapsed.

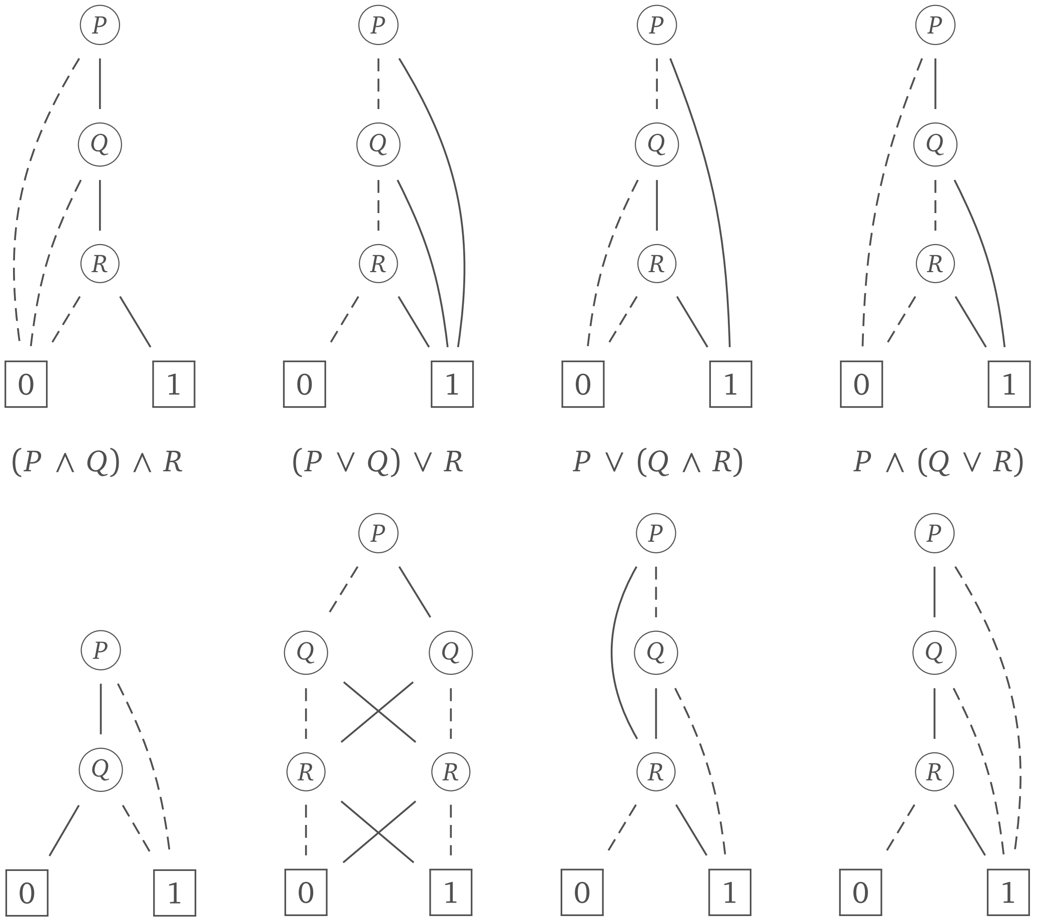
2. Verify these equivalences using BDDs.

$$(P \land Q) \land R \simeq P \land (Q \land R) \qquad (P \lor Q) \lor R \simeq P \lor (Q \lor R)$$

$$P \lor (Q \land R) \simeq (P \lor Q) \land (P \lor R) \qquad P \land (Q \lor R) \simeq (P \land Q) \lor (P \land R)$$

$$\neg(P \land Q) \simeq \neg P \lor \neg Q \qquad (P \leftrightarrow Q) \leftrightarrow R \simeq P \leftrightarrow (Q \leftrightarrow R)$$

$$(P \lor Q) \to R \simeq (P \to R) \land (Q \to R) \qquad (P \land Q) \to R \simeq P \to (Q \to R)$$

> Since the purpose of BDDs is that they are canonical representations of propositional formulae, the BDDs generated from both sides of the equivalences will be identical (and will only be shown once below). The method of constructing the BDDs will usually differ, however, so it is a good practice opportunity to go through the process of building both diagrams independently.
>
> 
>
>
> $(P \land Q) \land R$ $(P \lor Q) \lor R$ $P \lor (Q \land R)$ $P \land (Q \lor R)$
>
> $\neg(P \land Q)$ $(P \leftrightarrow Q) \leftrightarrow R$ $(P \lor Q) \to R$ $(P \land Q) \to R$

11. Modal logics

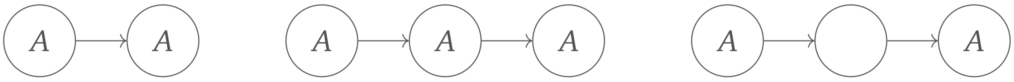
1. Explain why adding the T, 4 and B axioms make the transition relation reflexive, transitive and symmetric, respectively? Consider both the informal meaning and the formal semantics.

> We first consider a reflexive/transitive/symmetric frame and show that it must satisfy the respective axioms.
>
> **Reflexivity** $\to T$. Let (W,R) be a reflexive modal frame: for all $w \in W$, $(w,w) \in R$. We show that $\models_{W,R} \Box A \to A$. Take a world $w \in W$ and assume $w \Vdash \Box A$; that is, $v \Vdash A$ for all $w \in W$ such that $R(w,v)$. Since R is reflexive, one of the successor worlds must be w itself, so we also have $w \Vdash A$. Put together, this implies $w \Vdash \Box A \to A$ for an arbitrary w, so in fact $\models_{W,R} \Box A \to A$ as required.

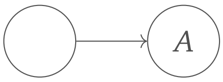
Transitivity $\rightarrow 4$. Let (W,R) be a transitive modal frame and assume $w \Vdash \Box A$ for a world $w \in W$. We need to show that $w \Vdash \Box\Box A$; that is, for all $v \in W$ for which $R(w,v)$, and for all $u \in W$ for which $R(v,u)$, we have $u \Vdash A$. Take such $v,u \in W$ satisfying $R(w,v)$ and $R(v,u)$. Since R is transitive, we also have $R(w,u)$, and combining this with the assumption $w \Vdash \Box A$, we have that $u \Vdash A$, as required.

Symmetry $\rightarrow B$. Let (W,R) be a symmetric modal frame and assume $w \Vdash A$ for a world $w \in W$. We need to show that $w \Vdash \Box\Diamond A$; that is, for every $u \in W$ with $R(w,u)$ there exists a $v \in W$ with $R(u,v)$ satisfying $w \Vdash A$. Take such an arbitrary $u \in W$ satisfying $R(w,u)$. Since R is symmetric, we also have $R(u,w)$, and by assumption $w \Vdash A$, so it serves as the required witness of existence.

The converse direction is a bit more subtle, especially since it is quite easy to come up with examples that seemingly violate the statements. For example, all states in the following three frames satisfy T, 4 and B respectively, but the corresponding frames are not reflexive, transitive, or symmetric:



The key point to recognise, however, is the following: when we say that T, 4 or B are *axioms* in a modal frame, we mean that they are satisfied in any world and *under any interpretation*. That is, given a frame (W,R), it satisfies axiom T if $\models_{W,R} \Box A \rightarrow A$, which, by definition, means that $\models_{W,R,I} \Box A \rightarrow A$ under any interpretation I. The above "counterexample" only satisfies T under a particular assignment, but one can find an assignment where T does not hold in every world:



Consequently, we cannot say that our frame (W,R) satisfies T so whether R is reflexive or not is irrelevant. The only way to ensure that a frame satisfies T no matter what assignment we choose is to make it reflexive. This flexibility over the interpretation is a crucial requirement for the converse proofs.

$T \rightarrow$ **Reflexivity**. Let (W,R) be a frame and assume $\models_{W,R} \Box A \rightarrow A$; that is, under all interpretations I and in all worlds $w \in W$, $w \Vdash \Box A \rightarrow A$. We need to show that R is reflexive, that is, for all $w \in W$, $R(w,w)$ holds. Take an arbitrary world $w \in W$, and for contradiction, assume that there is no transition from w to itself. Consider the interpretation $I_R(A) = W \setminus \{w\}$: A holds in all worlds except w. By the initial assumption, we have that if $w \Vdash \Box A$ then $w \Vdash A$ under the interpretation I_R, and we indeed have $w \Vdash \Box A$ since every world that w can transition to (which can only be states other than w since $\neg R(w,w)$) satisfies A. But then $w \Vdash A$ due to the axiom T, which is a contradiction since our assignment of A specifically excluded w. Thus, there must be a loop $R(w,w)$ for any w, proving that the frame is reflexive.

> $4 \to$ **Transitivity**. Let (W,R) be a frame and assume $\vDash_{W,R} \Box A \to \Box\Box A$. We need to prove that for all $w,v,u \in W$, if $R(w,v)$ and $R(v,u)$ then $R(w,u)$. Take such worlds $w,v,u \in W$ with $R(w,v)$ and $R(v,u)$ and for contradiction assume that $\neg R(w,u)$. Consider the interpretation $I_T(A) = W \setminus \{u\}$. By the initial assumption, we have that if $w \Vdash \Box A$ then $w \Vdash \Box\Box A$ under I_T, and we indeed have $w \Vdash \Box A$ since all the worlds that w can transition into (which does not include u by the assumption $\neg R(w,u)$) satisfy A. Then, by 4, we have $w \Vdash \Box\Box A$, which implies that u must satisfy A, contradicting our initial assumption. Since we reach a contradiction from $\neg R(w,u)$, we can conclude that R must be transitive.
>
> $B \to$ **Symmetry**. Let (W,R) be a frame and assume $\vDash_{W,R} A \to \Box\Diamond A$. We need to prove that for all $w,v \in W$, if $R(w,v)$ then $R(v,w)$. Take such worlds $w,v \in W$ with $R(w,v)$ and for contradiction assume that $\neg R(v,w)$. Consider the interpretation $I_S(A) = W \setminus \{u \in W \mid R(v,u)\}$: A holds in every state other than the ones v can transition to. Since by assumption $\neg R(v,w)$, we have that $w \Vdash A$, and by the axiom B, this implies $w \Vdash \Box\Diamond A$. However, this in particular means that there must be a state that u transitions to satisfying A, which contradicts our original assumption on I_S; thus, it can't be the case that $\neg R(v,w)$ so R must be symmetric.

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 $\Box\Box A \simeq \Box A$?

> We have the de Morgan duality $\neg\Box A \simeq \Diamond\neg A$ for modalities, which means every $\Box$ can be expressed as $\neg\Diamond\neg$ and vice versa. Rewriting a string of modalities in such a way results in a dual string of modalities separated by pairs of negations and "bookended" by a single negation on each side. The double negations cancel out, and so do the negations on the ends. For example, the equivalence $\Box\Box A \simeq \Box A$ translates to $\neg\Diamond\neg\neg\Diamond\neg A \simeq \neg\Diamond\neg A$ for all A, which simplifies to $\neg\Diamond\Diamond\neg A \simeq \neg\Diamond\neg A$. Negation preserves equivalences, so we have $\Diamond\Diamond\neg A \simeq \Diamond\neg A$, and this is merely the equivalence $\Diamond\Diamond B \simeq \Diamond B$ for $B = \neg A$.

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 $\Diamond(A \lor B) \simeq \Diamond A \lor \Diamond B$.

> Removing $\Diamond$ on the right is safe, so the applications of $(\Diamond r)$ and $(\lor l)$ can be permuted.
>
> $$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow A, \Diamond B}}{A \Rightarrow \Diamond A, \Diamond B}\,(\Diamond r) \qquad \dfrac{\dfrac{}{B \Rightarrow \Diamond A, B}}{B \Rightarrow \Diamond A, \Diamond B}\,(\Diamond r)}{A \lor B \Rightarrow \Diamond A, \Diamond B}\,(\lor l)}{\Diamond(A \lor B) \Rightarrow \Diamond A, \Diamond B}\,(\Diamond l)$$
>
> There is no flexibility in the converse case, since removing the $\Diamond$ on the right too early would prevent us from being able to safely remove $\Diamond$ on the left.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow A, B}}{A \Rightarrow A \lor B}\,(\lor r)}{A \Rightarrow \Diamond(A \lor B)}\,(\Diamond r)}{\Diamond A \Rightarrow \Diamond(A \lor B)}\,(\Diamond l) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{B \Rightarrow A, B}}{B \Rightarrow A \lor B}\,(\lor r)}{B \Rightarrow \Diamond(A \lor B)}\,(\Diamond r)}{\Diamond B \Rightarrow \Diamond(A \lor B)}\,(\Diamond l)}{\Diamond A \lor \Diamond B \Rightarrow \Diamond(A \lor B)}\,(\lor l)$$

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

First we prove $\Box(A \land B) \Rightarrow \Box A \land \Box B$, which is a dual of $\Diamond A \lor \Diamond B \Rightarrow \Diamond(A \lor B)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \Rightarrow A}}{A \land B \Rightarrow A}\,(\land l)}{\Box(A \land B) \Rightarrow A}\,(\Box l)}{\Box(A \land B) \Rightarrow \Box A}\,(\Box r) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A, B \Rightarrow B}}{A \land B \Rightarrow B}\,(\land l)}{\Box(A \land B) \Rightarrow B}\,(\Box l)}{\Box(A \land B) \Rightarrow \Box B}\,(\Box r)}{\Box(A \land B) \Rightarrow \Box A \land \Box B}\,(\land r)$$

Next, we prove $\Box A, \Box B \Rightarrow \Box(A \land B)$, which is a dual of $\Diamond(A \lor B) \Rightarrow \Diamond A, \Diamond B$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, \Box B \Rightarrow A}}{\Box A, \Box B \Rightarrow A}\,(\Box l) \qquad \dfrac{\dfrac{}{\Box A, B \Rightarrow B}}{\Box A, \Box B \Rightarrow B}\,(\Box l)}{\Box A, \Box B \Rightarrow A \land B}\,(\land r)}{\Box A, \Box B \Rightarrow \Box(A \land B)}\,(\Box r)$$

4. Prove the following sequents.

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

The first step performed must be $(\Diamond l)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow \Diamond B, A}}{\Box A \Rightarrow \Diamond B, A}\,(\Box l) \qquad \dfrac{\dfrac{}{B, \Box A \Rightarrow B}}{B, \Box A \Rightarrow \Diamond B}\,(\Diamond r)}{A \to B, \Box A \Rightarrow \Diamond B}\,(\to l)}{\Diamond(A \to B), \Box A \Rightarrow \Diamond B}\,(\Diamond l)$$

The second problem is tricky and requires careful attention to the order in which the modal operators are tackled. To avoid losing information, the critical rules are only applied when every formula on the left begins with a box, and every formula on the right begins with a diamond (in both cases excluding the formula directly affected by the rule. It is especially important to avoid batch-applying rules involving modalities, since applying a rule with a side-condition may remove propositions that we expect to be able to operate on later.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, \Box B \Rightarrow A}}{\Box A, \Box B \Rightarrow A}\,(\Box l) \qquad \dfrac{\dfrac{}{\Box A, B \Rightarrow B}}{\Box A, \Box B \Rightarrow B}\,(\Box l)}{\Box A, \Box B \Rightarrow A \wedge B}\,(\wedge r)}{\Box A, \Box B \Rightarrow \Box(A \wedge B)}\,(\Box r)}{\Box A, \Box B \Rightarrow \Diamond\Box(A \wedge B)}\,(\Diamond r)}{\Box A, \Diamond\Box B \Rightarrow \Diamond\Box(A \wedge B)}\,(\Diamond l)}{\Box A, \Box\Diamond\Box B \Rightarrow \Diamond\Box(A \wedge B)}\,(\Box l)}{\Diamond\Box A, \Box\Diamond\Box B \Rightarrow \Diamond\Box(A \wedge B)}\,(\Diamond l)}{\Box\Diamond\Box A, \Box\Diamond\Box B \Rightarrow \Diamond\Box(A \wedge B)}\,(\Box l)}{\Box\Diamond\Box A, \Box\Diamond\Box B \Rightarrow \Box\Diamond\Box(A \wedge B)}\,(\Box r)$$

12. Tableaux-based methods

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

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

$$(\exists y.\, \forall x.\, R(x, y)) \to (\forall x.\, \exists y.\, R(x, y))$$

We negate and convert to NNF:

$$\neg((\exists y.\, \forall x.\, R(x, y)) \to (\forall x.\, \exists y.\, R(x, y))) \simeq (\exists y.\, \forall x.\, R(x, y)) \wedge (\exists x.\, \forall y.\, \neg R(x, y))$$

We are using the free-variable tableau calculus, so we must Skolemise by replacing the two existentials with Skolem constants:

$$(\forall x.\, R(x, a)) \wedge (\forall y.\, \neg R(b, y))$$

Finally, we put this on the LHS of a sequent and derive a contradiction:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{w \mapsto b, v \mapsto a}}{R(w, a), \neg R(b, v) \Rightarrow}}{R(w, a), \forall y.\, \neg R(b, y) \Rightarrow}\,(\forall l, u/y)}{\forall x.\, R(x, a), \forall y.\, \neg R(b, y) \Rightarrow}\,(\forall l, w/x)}{(\forall x.\, R(x, a)) \wedge (\forall y.\, \neg R(b, y)) \Rightarrow}\,(\wedge l)$$

For

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

we negate, convert to NNF and Skolemise:

$$\begin{aligned} &\neg((P(a,b) \vee \exists z.\, P(z,z)) \to \exists x,y.\, P(x,y)) \\ \simeq\ &(P(a,b) \vee \exists z.\, P(z,z)) \wedge (\forall x.\, \forall y.\, \neg P(x,y)) && \text{(negate)} \\ \Longrightarrow\ &(P(a,b) \vee P(c,c)) \wedge (\forall x.\, \forall y.\, \neg P(x,y)) && \text{(Skolemise)} \end{aligned}$$

where c is a new Skolem constant.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{u_1 \mapsto a, w_1 \mapsto b}}{P(a,b),\ \neg P(u_1,w_1) \Rightarrow}}{P(a,b),\ \forall y.\, \neg P(u_1,y) \Rightarrow}\,(\forall l, w_1/y)}{P(a,b),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}\,(\forall l, u_1/x) \qquad \dfrac{\dfrac{\dfrac{\overline{u_2 \mapsto c, w_2 \mapsto c}}{P(c,c),\ \neg P(u_2,w_2) \Rightarrow}}{P(c,c),\ \forall y.\, \neg P(u_2,y) \Rightarrow}\,(\forall l, w_2/y)}{P(c,c),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}\,(\forall l, u_2/x)}{\dfrac{P(a,b) \vee P(c,c),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}{(P(a,b) \vee P(c,c)) \wedge (\forall x.\, \forall y.\, \neg P(x,y)) \Rightarrow}\,(\wedge l)}\,(\vee l)$$

For

$$((\exists x.\, P(x)) \to Q) \to (\forall x.\, P(x) \to Q)$$

we negate, convert to NNF and Skolemise:

$$\begin{aligned} &\neg(((\exists x.\, P(x)) \to Q) \to (\forall x.\, P(x) \to Q)) \\ \simeq\ &((\forall x.\, \neg P(x)) \vee Q) \wedge (\exists x.\, P(x) \wedge \neg Q) && \text{(negate)} \\ \Longrightarrow\ &((\forall x.\, \neg P(x)) \vee Q) \wedge P(a) \wedge \neg Q && \text{(Skolemise)} \end{aligned}$$

Separating the conjunctions and placing on the LHS of a sequent, we get

$$\dfrac{\dfrac{\dfrac{\overline{u \mapsto a}}{\neg P(u),\ P(a),\ \neg Q \Rightarrow}}{\forall x.\, \neg P(x),\ P(a),\ \neg Q \Rightarrow}\,(\forall l, u/x) \qquad \dfrac{}{Q,\ P(a),\ \neg Q \Rightarrow}}{(\forall x.\, \neg P(x)) \vee Q,\ P(a),\ \neg Q \Rightarrow}\,(\vee l)$$

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

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

Sequent calculus. A proof system for direct proof: the formula is placed on the RHS of the sequent without any alterations, and one follows the syntax-directed connective- and quantifier-introduction rules to reach the basic sequent $\Gamma, A \Rightarrow A, \Delta$, representing the conclusion of A from an assumption of A. While sequent calculus requires no preprocessing of the formula (negation or conversion to a normal form), the proof algorithm is more complicated due to it needing to handle all possible logical connectives both in the assumption and the goal context. The $(\exists l)$ and $(\forall r)$ quantifier rules impose side conditions on the freshness of variable names, while $(\forall l)$ and $(\exists r)$ require one to find appropriate witness terms and instantiations in the middle of a proof. Since we may not be able to know what particular instance or witness will be needed, these steps may require educated guessing and backtracking.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(a,b) \Rightarrow P(a,b)}}{P(a,b) \Rightarrow \exists y.\, P(a,y)}\;(\exists r, b/y)}{P(a,b) \Rightarrow \exists x, y.\, P(x,y)}\;(\exists r, a/x) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{P(z,z) \Rightarrow P(z,z)}}{P(z,z) \Rightarrow \exists y.\, P(z,y)}\;(\exists r, z/y)}{P(z,z) \Rightarrow \exists x, y.\, P(x,y)}\;(\exists r, z/x)}{\exists z.\, P(z,z) \Rightarrow \exists x, y.\, P(x,y)}\;(\exists l)}{(P(a,b) \vee \exists z.\, P(z,z)) \Rightarrow \exists x, y.\, P(x,y)}\;(\vee l)}{\Rightarrow (P(a,b) \vee \exists z.\, P(z,z)) \rightarrow \exists x, y.\, P(x,y)}\;(\rightarrow r)$$

Resolution. A refutation proof technique for establishing validity: we show that the negation of a formula is unsatisfiable. Resolution does away with the complicated and rigid sequent calculus framework in favour of a single inference rule applied to a normalised representation of the problem. The formula is first negated, then converted to conjunctive normal form, also known as clausal form. Existentially quantified variables are eliminated using Skolemisation, and universal quantifiers are left implicit. The resolution rule makes hypothetical inferences amongst the clauses, aiming to reach the empty clause that denotes a contradiction. Instantiation of variables is done via unification, ensuring that instance search is never done "blindly". The main drawback is that CNF conversion is error-prone when done by hand, and may well result in exponential blow-up in the number of clauses – often most of the work of a resolution proof happens in this normalisation step.

Conversion of the formula to clausal form has already been demonstrated above:

$$(P(a,b) \vee P(c,c)) \wedge (\forall x.\, \forall y.\, \neg P(x,y))$$

In clausal form, this is:

$$① \ \{P(a,b), P(c,c)\} \qquad ② \ \{\neg P(x,y)\}$$

We resolve the two clauses on $P(a,b)$, unifying x with a and y with b to get $\{P(c,c)\}$, then resolve this new clause with ② again (unifying both x and y with c) to reach the empty clause.

Free-variable tableau calculus. We combine two favourable aspects of the sequent and resolution techniques: limited preprocessing and natural reasoning steps on the one hand, and a small set of inference rules and streamlined handling of variables on the other. Free-variable tableau calculus is also a contradiction-based proof technique, so the formula is first negated and converted to negation normal form. This eliminates implication and pushes negation to atomic formulae, but does not distribute conjunctions over disjunctions. The reduced number of connectives means that we do not require a large number of sequent rules: the left introductions for disjunction, conjunction, and universal quantification suffice. The basic sequent becomes $\Gamma, A, \neg A \Rightarrow$, expressing a contradiction. Free-variable tableaux avoid unguided instance search for the $(\forall l)$ rule by replacing universally quantified variables with fresh ones, and instantiating them at the very end with unification. To do this, the NNF formula must also be Skolemised, otherwise we could not differentiate between the $(\exists l)$ and $(\forall l)$ rules.

The tableaux proof of the formula has already been demonstrated above; the important differences with the normal sequent proof is that instantiation of the variables is deferred until the very end.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{u_1 \mapsto a, w_1 \mapsto b}}{P(a,b),\ \neg P(u_1,w_1) \Rightarrow}}{P(a,b),\ \forall y.\, \neg P(u_1,y) \Rightarrow}\,(\forall l, w_1/y)}{P(a,b),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}\,(\forall l, u_1/x) \qquad \dfrac{\dfrac{\dfrac{\overline{u_2 \mapsto c, w_2 \mapsto c}}{P(c,c),\ \neg P(u_2,w_2) \Rightarrow}}{P(c,c),\ \forall y.\, \neg P(u_2,y) \Rightarrow}\,(\forall l, w_2/y)}{P(c,c),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}\,(\forall l, u_2/x)}{P(a,b) \lor P(c,c),\ \forall x.\, \forall y.\, \neg P(x,y) \Rightarrow}\,(\lor l)}{(P(a,b) \lor P(c,c)) \land (\forall x.\, \forall y.\, \neg P(x,y)) \Rightarrow}\,(\land l)$$

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 $\neg\Box\neg A$.

In some cases the duality is self-evident and can be expressed using appropriate pairs of English words. In other cases (namely belief and knowledge) a bit more thinking is required; we are essentially trying to capture being “indifferent” to the proposition, i.e. that we are not going to argue against it if it is proposed to be true. This is suitably between affirming and denying the proposition, which is what $\Diamond$ intends to express.

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

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) $\Box A \to \Diamond A$

> **Distribution**: $\Box(A \to B) \land \Box A \to \Box B$. This is nothing but the ("uncurried" form of) axiom K, assumed to hold in every modal logic.
>
> **Reflexivity**: $\Box A \to A$.
>
> - *Time*: we assume that the future includes the present, so if $\Box A$ holds at a current "time step" (world) we must also have A.
> - *Necessity*: necessary truth is stronger than simple truth.
> - ~~*Belief*~~: most definitely not reflexive: believing something doesn't make it true.
> - *Knowledge*: the difference between knowledge and belief is that (ideally) knowing something to be true means it must be true; presumably the only way to know a proposition to be true is to have proof or irrefutable evidence for it.
> - ~~*Duty*~~: in an ideal world, maybe – but there will always be rule-breakers, so obligatory things are not necessarily true.
>
> **Transitivity**: $\Box A \to \Box\Box A$.
>
> - *Time*: if something holds always in the future, this will also be case at any point in the future.
> - *Necessity*: necessary things are necessarily necessary – logical laws are assertions whose truth cannot be denied. However, if we're talking about physical, rather than logical necessity, transitivity would mean that the physical laws themselves entail that they should be laws of the universe, which is more questionable.
> - *Belief and knowledge*: transitivity represents positive introspection: if I know something to be true, I know that I know it to be true[a]. Negative introspection $\neg\Box A \to \Box\neg\Box A$ would then be "if I don't know A, I know that I don't know A" or "I am aware of the limits of my knowledge".
>
> [a] Epistemic analysis of *Friends* S05E14 anyone?

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?