universität innsbruck

Computational Logic	SS 2020	703824 VU

TAKE HOME EXAM — May 12, 9:00 – May 13, 9:00, 2020[1]

There are 42 points available, plus 4 bonus points. The points scored are added to the crosses of the assignments and divided by 0.82 to determine your percentage for the course. You need at least 50 percent to pass.

$\boxed{1}$ This exercise is about first-order logic. Consider the first-order formula $\varphi = (\forall x)(\exists y)[P(x) \supset Q(y)] \supset (\forall x)[P(a) \supset (\exists y)Q(y)]$ with a a constant. It is a tautology.

[4] (a) First stepwise compute a prenex form φ' of φ, in each step giving the quantifier rewrite rule employed, and next Skolemize φ', per quantifier, to obtain a formula φ''.

Answer: $(\forall x)(\exists y)[P(x) \supset Q(y)] \supset (\forall x)[P(a) \supset (\exists y)Q(y)]$ transforms (since the right $\forall x$ does not bind) to $(\forall x)(\exists y)[P(x) \supset Q(y)] \supset [P(a) \supset (\exists y)Q(y)]$, next (pulling the right positively occurring $\exists y$ out) to $(\exists y)((\forall x)(\exists y)[P(x) \supset Q(y)] \supset [P(a) \supset Q(y)])$, then (pulling negatively occurring $\forall x$ out) to $(\exists y)(\exists x)((\exists y)[P(x) \supset Q(y)] \supset [P(a) \supset Q(y)])$, and finally (pulling negatively occurring $\exists y$ out, renaming to z to avoid capture) to $(\exists y)(\exists x)(\forall z)([P(x) \supset Q(z)] \supset [P(a) \supset Q(y)])$.

Skolemising $\exists y$ yields $(\exists x)(\forall z)([P(x) \supset Q(z)] \supset [P(a) \supset Q(b)])$, and then Skolemising $\exists x$ yields the final result $(\forall z)([P(c) \supset Q(z)] \supset [P(a) \supset Q(b)])$.

Note that different prenex forms are possible. The one constructed above gives the minimal number of dependencies (of $\exists$s on $\forall$s), namely no such dependencies, hence the smallest Skolemised result (only constants, b, c, are introduced).

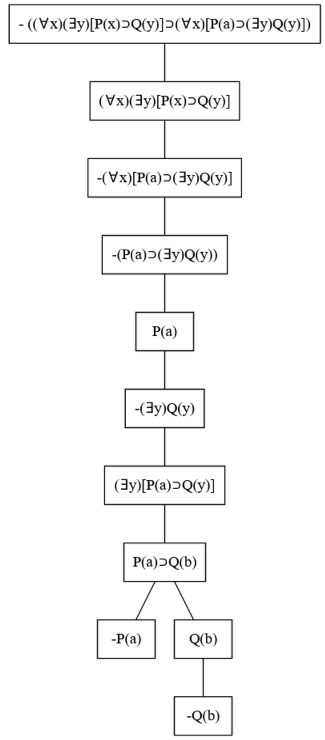
[3] (b) Consider the singleton set $S = \{\varphi\}$. Give a Herbrand model of S (Herbrand with respect to the original first-order language of φ extended with parameters).

Answer: a Herbrand model is a model $\langle D, I\rangle$ having as domain D the closed terms over the constants and function symbols. Since here we only have constants, namely a and an infinite set of parameters, D comprises exactly those constants (as terms). Moreover, in a Herbrand model, terms/constants are interpreted as themselves. Hence it only remains to interpret the predicate symbols, P and Q, which we both may interpret arbitrarily (the formula is a tautology) for instance as the empty set, i.e. $P^I = Q^I = \emptyset$ (vacuously satisfying both sides of the main implication of φ, hence the formula itself).

[4] (c) Give a tableau proof of φ.

Answer:

[1] Times in CEST



[12] $\boxed{2}$ This exercise is about proofs. Answer $\boxed{\textbf{three}}$ of the following five items (4 points per item).

(a) Prove that if X and Y are propositional formulas that are *equivalent*, i.e. $v(X \equiv Y) = \mathbf{t}$ for all valuations v, then their duals X^d and Y^d are equivalent too. Illustrate this for $X = P \vee (\neg Q \wedge R)$ and $Y = (P \vee \neg Q) \wedge (P \vee R)$.

Answer: We use from Exc. 2.4.11 that $v(X^d) = v(\neg\overline{X})$ for all valuations v, where $\overline{X}$ is obtained from X by negating all occurrences of propositional letters in it. Then $X \equiv Y$ is a tautology iff (by Exc. 2.4.10) $\overline{X \equiv Y}$ is a tautology iff (by def. of overlining) $\overline{X} \equiv \overline{Y}$ is a tautology iff (since $(\neg X') \equiv Y'$ is equivalent to $\neg(X' \equiv Y')$, $X' \equiv Y'$ to $Y' \equiv X'$ and $\neg\neg X'$ to X') $\neg\overline{X} \equiv \neg\overline{Y}$ is a tautology iff (by Exc. 2.4.11) $X^d \equiv Y^d$ is a tautology.

The above was also explained intuitively in the lecture, namely by that the truth table of X^d is obtained by flipping the truth table of X upside-down (corresponding to $\overline{(\,\cdot\,)}$) and inverting the values (corresponding to $\neg(\,\cdot\,)$). From this it is obvious that if X and Y are equivalent, they have the same truth table, hence flipping and inverting both, the resulting truth tables of X^d and Y^d are the same again (and vice versa).

For the example X and Y, which are equivalent since the latter is obtained by distributivity from the former, the duals are $X = P \wedge (\neg Q \vee R)$ and $Y = (P \wedge \neg Q) \vee (P \wedge R)$, as computed simply by swapping occurrences of $\wedge$s and $\vee$s ($\neg$ is self-dual)., which are equivalent by distributivity again (but now of $\wedge$ over $\vee$ instead of of $\vee$ over $\wedge$).

(b) Suppose we change the 4th clause of the definition of propositional Hintikka set (Definition 3.5.1) in the following way:

4. $\alpha \in \mathbf{H} \Rightarrow \alpha_1 \in \mathbf{H}$

giving rise (combined with the other, unchanged, clauses) to what we will call *Hintikka'* sets. The notion of Hintikka' set is not a good one. Give a relevant property (for showing completeness results) that Hintikka sets have, and show (how) it fails for Hintikka' sets.

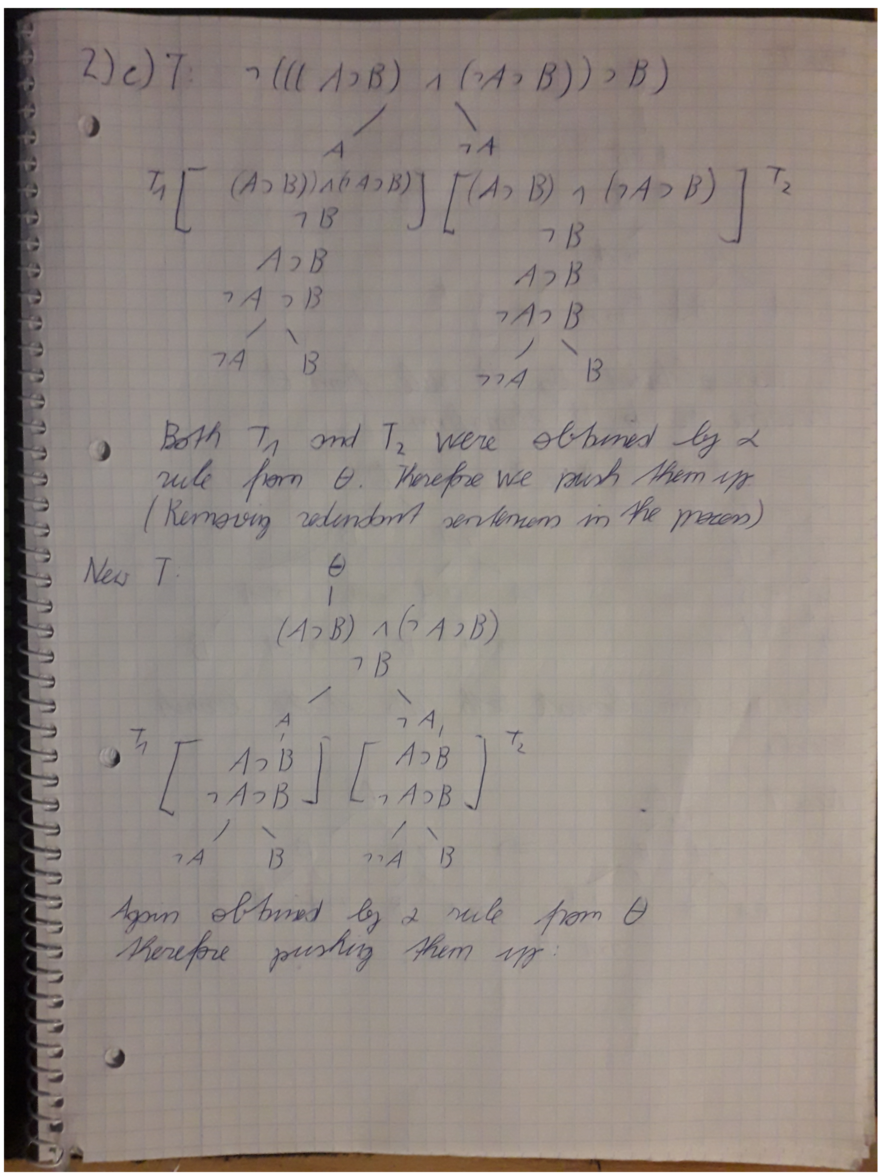
Answer: For example, Hintikka's Lemma (Proposition 3.5.2) fails for Hintikka' sets. That is, propositional Hintikka' sets need not be satisfiable. For instance $\{a \wedge \neg a, a\}$ is a Hintikka' set, but is not satisfiable, since $a \wedge \neg a$ on its own is already a contradiction. Note that this is not a Hintikka set since $a \wedge \neg a$ being a member would then enforce by clause 4 that also $\neg a$ be in the set. (Note that adjoining $\neg a$ would not result in a Hintikka set either as we then clause 1 would be violated; indeed this set being unsatisfiable, it cannot be extended to any Hintikka set.)

(c) Transform the following tableau into a *cut-free* tableau using the cut-elimination procedure from the lecture/book:

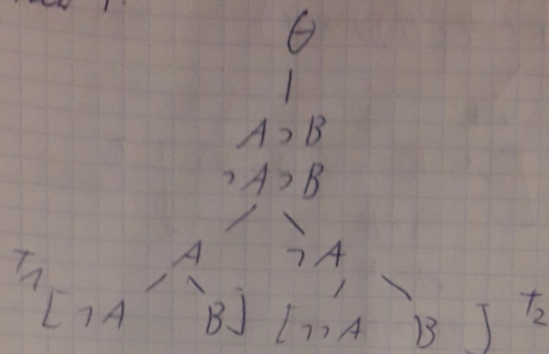
$$\neg(((A \supset B) \wedge (\neg A \supset B)) \supset B)$$

A	$\neg A$
$(A \supset B) \wedge (\neg A \supset B)$	$(A \supset B) \wedge (\neg A \supset B)$
$\neg B$	$\neg B$
$A \supset B$	$A \supset B$
$\neg A \supset B$	$\neg A \supset B$
$\neg A$ | B	$\neg\neg A$ | B

Answer:



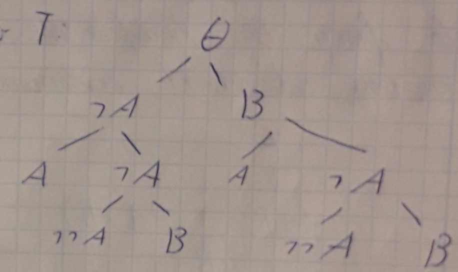
New T:



T_1 was obtained by B rule from θ therefore we do B transform

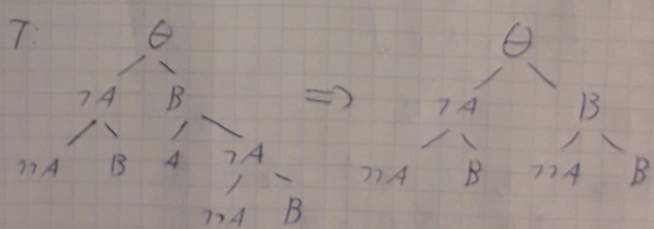
$B_1 := \neg A$
$B_2 := B$
$T_2' := T_2$
$T_1' := \{\}$
$T_1^K := \{\}$

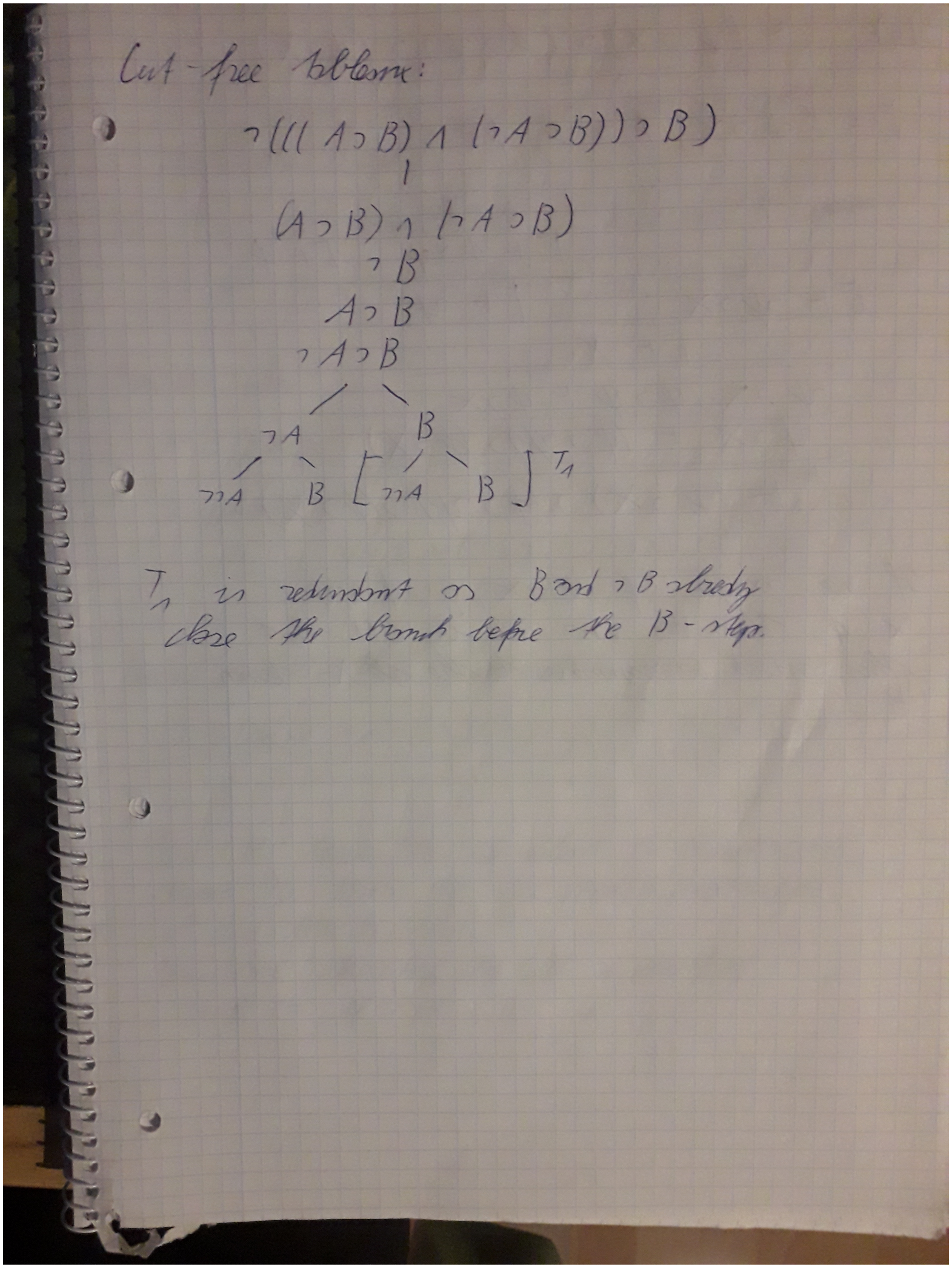
New T:



Now we can eliminate both cuts at the branch ends

New T:




Cut-free tableau:

$\neg(((A \supset B) \wedge (\neg A \supset B)) \supset B)$

$(A \supset B) \wedge (\neg A \supset B)$

$\neg B$

$A \supset B$

$\neg A \supset B$

$\neg A \qquad B$

$\neg\neg A \quad B \quad \left[\neg\neg A \quad B\right] T_1$

T_1 is redundant as B and $\neg B$ already close the branch before the B-step.

(d) Consider the propositional formulas $\varphi = \neg P \supset (P \supset \bot)$ and $\varphi' = (P \supset \bot) \supset \neg P$. Give proofs of φ and φ' using the 9 Axiom Schemes and MP of the Hilbert System of Fitting. (Recall that in Fitting, $\neg P$ is *not* an abbreviation of $P \supset \bot$.)

Answer: A HS proof of φ:

i. $P \supset (\neg P \supset \bot)$ (AS 6)

ii. $(P \supset (\neg P \supset \bot)) \supset (\neg P \supset (P \supset \bot))$ (Exc. 4.1.1)

iii. $\neg P \supset (P \supset \bot)$ (MP ii,i)

A HS proof of φ':

i. $(\neg P \supset \neg P) \supset ((\bot \supset \neg P) \supset ((P \supset \bot) \supset \neg P))$ (AS 9)
ii. $\neg P \supset \neg P$ (Example on page 80)
iii. $(\bot \supset \neg P) \supset ((P \supset \bot) \supset \neg P)$ (MP i,ii)
iv. $\bot \supset \neg P$ (AS 3)
v. $(P \supset \bot) \supset \neg P$ (MP iii,iv)

(e) Prove that for *maximal* states in a Kripke model (intuitionistic) forcing coincides with (classical) truth. Formally, let some Kripke mode be given and let c be *maximal* in it, i.e. for all c', if $c \leqslant c'$ then $c = c'$. Prove that if we define for all propositional letters $v(p) = \mathbf{t}$ if $c \Vdash p$, then for all propositional formulas ϕ constructed from propositional letters and $\supset, \bot, \vee, \wedge$, we have $v(\phi) = \mathbf{t}$ iff $c \Vdash \phi$. Illustrate this for the formula $((p \supset \bot) \supset \bot) \supset p$.

Answer: We prove $v(\phi) = \mathbf{t}$ iff $c \Vdash \phi$, by induction on ϕ. Since the classical and intuitionistic semantics of the connectives other than implication are the same (evaluated in the same world), they can be dealt with by (un)folding of the definitions and induction:

- If ϕ is a propositional letter p, the statement holds by definition of v;
- If ϕ is bottom $\bot$, then neither side holds by the semantics of valuations resp. forcing;
- If $\phi = \phi_1 \wedge \phi_2$, then $v(\phi_1 \wedge \phi_2) = \mathbf{t}$ iff (by the truth-table semantics of $\wedge$) $v(\phi_1) = \mathbf{t}$ and $v(\phi_2) = \mathbf{t}$ iff (by the IH for ϕ_1, ϕ_2) $c \Vdash \phi_1$ and $c \Vdash \phi_2$ iff (by the Kripke semantics of $\wedge$) $c \Vdash \phi_1 \wedge \phi_2$;
- If $\phi = \phi_1 \vee \phi_2$, we proceed as in the previous item, but replacing '$\wedge$' by '$\vee$', and 'and' by 'or'.

The interesting case is implication: If $\phi = \phi_1 \supset \phi_2$, then $v(\phi_1 \supset \phi_2) = \mathbf{t}$ iff if $v(\phi_1) = \mathbf{t}$ then $v(\phi_2) = \mathbf{t}$ iff if $c \Vdash \phi_1$ then $c \Vdash \phi_2$ iff (by maximality of c) for all c' such that $c \leqslant c'$, if $c' \Vdash \phi_1$ then $c' \Vdash \phi_2$ iff $c \Vdash \phi_1 \supset \phi_2$. The basic intuition is that if 'the future = the present' then reasoning about the future is the same as reasoning about the present. From this we can conclude that the formula $((p \supset \bot) \supset \bot) \supset p$ is forced (intuitionistically) in any maximal world since it is a (classical) tautology, although there may be (non-maximal) worlds where it is not forced.

$\boxed{3}$ This exercise is about the Curry–Howard isomorphism. Let B be the λ-term $\lambda f\, g\, x. f\, (g\, x)$

[3] (a) Give the ND proof (in tree form) of $(\psi \supset \chi) \supset (\phi \supset \psi) \supset (\phi \supset \chi)$ for all propositional formulas ϕ, ψ, χ, corresponding to the λ-term B.

Answer: Using the Curry–Howard isomorphism (slide 24 of lecture 8), the ND tree is obtained from the tree on slide 15 of lecture 8, by simply omitting the terms (and the following colon),

[4] (b) Show that, for all propositional formulas ϕ, $\phi \supset \phi$ can be proven indirectly by using B. More precisely, first show that $\vdash B\,(\lambda x.x)\,(\lambda x.x) : \tau \to \tau$ for all simple types τ and that that gives an ND proof that $\phi \supset \phi$ for all propositional formulas ϕ. Next, show that $B\,(\lambda x.x)\,(\lambda x.x)$ normalizes to $\lambda x.x$ (possibly up to renaming) by repeated uses of $\to_\beta$.

Answer: The ND proof corresponding to B of the previous item proving that $(\psi \supset \chi) \supset (\phi \supset \psi) \supset (\phi \supset \chi)$ for all propositional formulas ϕ, ψ, χ, in particular proves $(\phi \supset \phi) \supset (\phi \supset \phi) \supset (\phi \supset \phi)$ for all ϕ. That is, via Curry–Howard B can be assigned typez $(\tau \to \tau) \to (\tau \to \tau) \to (\tau \to \tau)$ for any simple type τ. Since we know (from the lecture) that $\vdash \lambda x.x : \tau \to \tau$ for all τ, two applications of former on the latter (twice) shows that $\vdash B\,(\lambda x.x)\,(\lambda x.x) : \tau \to \tau$, which, via Curry–Howard, yields a proof of $\phi \supset \phi$ for all propositional formulas ϕ.

Abbreviating $\lambda x.x$ to I, we compute $B\,I\,I \to_\beta (\lambda g\, x. I\,(g\, x))\, I \to_\beta (\lambda g\, x. g\, x)\, I \to_\beta \lambda x. I\, x \to_\beta I$, as desired.

[4] (c) The λ-term $\lambda x.x$ both behaves as the identity and has the type of the identity. Formally, both $(\lambda x.x)\,M \rightarrow_\beta^* M$ for every λ-term M and $\vdash \lambda x.x : \tau \rightarrow \tau$ for every simple type τ. Does every (closed) λ-term that has the type of the identity, behave as the identity? That is, prove or give a counterexample to that for every simply typed λ-term E, if $\vdash E : \tau \rightarrow \tau$ for every simple type τ, then $E\,M \rightarrow_\beta^* M$ for all λ-terms M.

Answer: This indeed holds, since, we claim, if $\vdash N : \tau \rightarrow \tau$ and N is in $\rightarrow_\beta$-normal form, then N is of shape $\lambda x.x$ Since an arbitrary term $\vdash E : \tau \rightarrow \tau$ can be normalised (by SN) with normal form having type $\tau \rightarrow \tau$ by subject reduction, that normal form must be of shape $\lambda x.x$, hence $E\,M \rightarrow_\beta^* (\lambda x.x)\,M \rightarrow_\beta M$, as desired.

The claim that N must be of shape $\lambda x.x$ follows from the subformula property (cf. the earlier assignment on $\tau \rightarrow \tau \rightarrow \tau$ having two inhabitants). Formally, if $\vdash N : \tau \rightarrow \tau$ and N is in normal form, then in its derivation only subformulas of $\tau \rightarrow \tau$ occur. In particular, if τ is of base type, then only $\tau \rightarrow \tau$ and τ may occur. Since N must be closed, it must be of shape $\lambda x.M$ for some variable x and term M to which type τ can be assigned, assuming x is assigned type τ. Since τ was assumed a base type, M cannot be an abstraction, so must (by the assumption that N is in normal form) be of shape $y\vec{P}$ for some variable y and term vector $\vec{P}$. x being the only variable available in the context $x = y$, hence $\vec{P}$ must be the empty vector by x being of base type τ. Hence $N = \lambda x.M = \lambda x.x$.

[4] (bonus) The CL-term $\mathsf{S\,K\,K}$ both behaves as the identity and has the type of the identity. Formally, both $\mathsf{S\,K\,K}\,M \rightarrow_w^* M$ for every CL-term M and $\vdash \mathsf{S\,K\,K} : \tau \rightarrow \tau$ for every simple type τ. Does every CL-term that behaves as the identity have the type of the identity? That is, prove or give a counterexample to that for every simply typed CL-term E, if $E\,M \rightarrow_w^* M$ for all CL-terms M, then $\vdash E : \tau \rightarrow \tau$ for every simple type τ.

Answer: Counterexample. Setting $E = K\,(S\,K\,K)\,y$ we have $E\,M \rightarrow_w S\,K\,K\,M \rightarrow_w^* M$ as required but not $\vdash E : \tau \rightarrow \tau$ for every simple type τ, simply because E is not closed.

Note that although subject reduction holds, i.e. that if a term M can be assigned some type τ in some context Γ, and $M \rightarrow_\beta^* M'$ then M' can also be assigned type τ in context Γ, going in the converse direction, expanding M' to M, may give rise to extra constraints on the context (as for E above) and to more restricted types (although $S\,K\,S\,x \rightarrow^* x$, the type of $S\,K\,S$ is not the identity type).

[8] $\boxed{4}$ Determine whether the following statements are true or false.

Every correct answer is worth 2 points. For every wrong answer 1 point is subtracted, provided the total number of points is non-negative.

(a) If $\mathcal{C}_1$ and $\mathcal{C}_2$ are propositional consistency properties, then their intersection $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$ is a propositional consistency property again.

Answer: No. Take for example $\mathcal{C}_i = \{\{a_1 \vee a_2, a_i\}\}$. Then $\mathcal{C} = \{\{a_1 \vee a_2\}\}$, which is not a propositional consistency property since condition 5 (of Definition 3.6.1 in Fitting) fails when considering $a_1 \vee a_2 \in \{a_1 \vee a_2\}$. One can already suspect failure just from the shape of the conditions. In particular, from that condition 5 uses an 'or' in it conclusion, requiring a choice to hold. The above example exploits this by letting $\mathcal{C}_1$ and $\mathcal{C}_2$ make different choices, leaving no choice in their intersection $\mathcal{C}$.

(b) In propositional logic, if Z, Z' are both interpolants of $X \supset Y$, then $Z \supset Z'$ is a tautology or $Z' \supset Z$ is a tautology (or both).

Answer: No. $Z = a$ and $Z' = b$ are both interpolants of $(a \wedge b) \supset (a \vee b)$, but neither $a \supset b$ nor $b \supset a$ is a tautology. One can already suspect failure just from the fact that although $\supset$ is a quasi-order (reflexive and transitive), it is not a total order.[2] The up-shot is that thinking of an interpolant of $X \supset Y$ as being in 'the middle' between X and Y is only an approximately useful intuition.

(c) If ϕ_1 and ϕ_2 are obtained by Skolemising (possibly distinct) prenex forms of the same first-order formula ϕ, then ϕ_1 and ϕ_2 have the same number of constants.

Answer: No. Take for example, $\phi = (\exists x)P(x) \wedge (\forall y)Q(y)$ having prenex forms both $\phi_1 = (\exists x)(\forall y)(P(x) \wedge Q(y))$ and $\phi_2 = (\forall y)(\exists x)(P(x) \wedge Q(y))$. Skolemising the $(\exists x)$ in the former introduces a constant whereas for the latter it introduces a function symbol (of arity 1, depending on y). The up-shot is that 'linearising' the quantifiers in a formula by pulling them out into a quantifier-prefix may *introduce* depedencies (which is typically bad for proof procedures).

(d) The formula $(\exists x)R(x, f(b)) \wedge (\exists y)R(a, y)$ is an interpolant of

$$(R(a, b) \wedge (\forall x)(\exists y)(R(a, x) \supset R(y, f(x)))) \supset (R(a, c) \vee (\exists x)R(x, f(b)))$$

Answer: Yes. It is easily seen that both respective implications are tautologies (e.g. by using tableaux).

[2] $(Z \supset Z') \vee (Z' \supset Z)$ *is* a tautology for any Z, Z' though in classical logic (but not in intuitionistic logic; cf. the disjunction property).