Exam

A number of different exercises is proposed. You do not need to try to solve them all.

Exercise 1 Let R be a relation on a set X, that is, a subset of X^2. Let R^0 be the identity relation, that is, x is in relation with y, written xR^0y, if $x = y$. And let R^{n+1} be the composition of R and R^n. The composition of two relations R and S, written $R \circ S$, is the relation such that $x(R \circ S)y$ if there is z such that xRz and zRy. Hence, xR^ny $(n > 0)$ if there are $n-1$ intermediate elements $x_1, \ldots, x_{n-1}$ such that $xRx_1, \ldots, x_{n-1}Ry$. A relation S is reflexive if, for all x, xSx. A relation S is transitive if, for all x, y, z, xSz whenever xSy and ySz. Prove that:

1. $R^+ = \bigcup_{i>0} R^i$ is transitive.
2. R^+ is the smallest transitive relation containing R.
3. $R^* = \bigcup_{i\geq 0} R^i$ is transitive and reflexive.
4. R^* is the smallest transitive and reflexive relation containing R.
5. The function $f(X) = X \circ X$ is monotone, that is, $f(X) \subseteq f(Y)$ if $X \subseteq Y$.
6. R^* is a fixpoint of f, that is, $f(R^*) = R^*$.

Proof.

1. Assume that xR^+y and yR^+z. Then, there are i and j such that xR^iy and yR^jz. Thus, $xR^{i+j}z$ and xR^+z.
2. Let S be a transitive relation containing R. We prove by induction on $i \geq 1$ that R^i is included in S. For $i = 1$, we have $R^1 = R \subseteq S$ by assumption. Assume now that $R^i \subseteq S$ and that $xR^{i+1}z$. Then, there is y such that xRy and yR^iz. Since $R \subseteq S$ and $R^i \subseteq S$, we have xSy and ySz. Since S is transitive, we have xSz. Thus, $R^{i+1} \subseteq S$.
3. For transitivity, the proof is the same as in 1. R^* is reflexive since it includes R^0.
4. As in 2 except that $i \geq 0$. In the case $i = 0$, $R^0 \subseteq S$ since S is reflexive.
5. Assume that aX^2c. Then, there is b such that aXb and bXc. Since $X \subseteq Y$, we have aYb and bYc. Thus, aY^2c.

6. We first prove that $f(R^*) \subseteq R^*$. Let $(x,z) \in f(R^*)$. Then, there is y such that xR^*y and yR^*z. Since R^* is transitive, xR^*z. We now prove that $R^* \subseteq f(R^*)$. Assume that xR^*y. Since R^* is reflexive, we have xR^*xR^*y and $(x,y) \in f(R^*)$.

Exercise 2 We consider the set of λ-terms $t = x \mid \lambda xt \mid tt$, where x is a variable taken in an infinite set $\mathcal{X}$. Let $\rightarrow_\beta$ be the smallest relation such that:

- $(\lambda xt)u \rightarrow_\beta t\{x \mapsto u\}$, where $t\{x \mapsto u\}$ is the term obtained by replacing every free occurrence of x in t by u (and renaming bound variables if necessary)
- $\lambda xt \rightarrow_\beta \lambda xt'$ if $t \rightarrow_\beta t'$
- $tu \rightarrow_\beta t'u$ if $t \rightarrow_\beta t'$
- $tu \rightarrow_\beta tu'$ if $u \rightarrow_\beta u'$

Prove that:

1. β-reduction introduces no new variables: if $t \rightarrow_\beta t'$, then $\mathrm{FV}(t') \subseteq \mathrm{FV}(t)$.
2. If $v \rightarrow_\beta^* v'$, then $t\{y \mapsto v\} \rightarrow_\beta^* t\{y \mapsto v'\}$.
3. $\rightarrow_\beta$ is stable by substitution: if $t \rightarrow_\beta t'$, then $t\{y \mapsto v\} \rightarrow_\beta t'\{y \mapsto v\}$.
4. $\rightarrow_\beta$ is locally confluent, that is, if $t \rightarrow_\beta u$ and $t \rightarrow_\beta v$, then there is w such that $u \rightarrow_\beta^* w$ and $v \rightarrow_\beta^* w$.

This last property means that, locally, the order in which we make β-reductions is not important, since we can always find a common reduct. An important property of β-reduction is that it also holds globally: if $t \rightarrow_\beta^* u$ and $t \rightarrow_\beta^* v$, then there is w such that $u \rightarrow_\beta^* w$ and $v \rightarrow_\beta^* w$. Thus, β-reduction is in some sense deterministic: it can lead to only one result.

Proof.

1. We proceed by induction on the definition of $\rightarrow_\beta$.
   - Case $(\lambda xt)u \rightarrow_\beta t\{x \mapsto u\}$. We have $\mathrm{FV}((\lambda xt)u) = (\mathrm{FV}(t) - \{x\}) \cup \mathrm{FV}(u)$. By renaming, we can assume that $x \notin \mathrm{FV}(u)$. Let $y \in \mathrm{FV}(t\{x \mapsto u\}$. Either $y \in \mathrm{FV}(u)$ and we are done, or $y \in \mathrm{FV}(t)$. But $y \neq x$ since $x \notin \mathrm{FV}(u)$ and every occurrence of x is replaced by u. Therefore, $y \in \mathrm{FV}((\lambda xt)u)$.
   - Case $\lambda xt \rightarrow_\beta \lambda xt'$ since $t \rightarrow_\beta t'$. We have $\mathrm{FV}(\lambda xt) = \mathrm{FV}(t) - \{x\}$ and $\mathrm{FV}(\lambda xt') = \mathrm{FV}(t') - \{x\}$. And by induction hypothesis, we have $\mathrm{FV}(t') \subseteq \mathrm{FV}(t)$. Therefore, $\mathrm{FV}(\lambda xt') \subseteq \mathrm{FV}(\lambda xt)$.
   - Case $tu \rightarrow_\beta t'u$ since $t \rightarrow_\beta t'$. We have $\mathrm{FV}(tu) = \mathrm{FV}(t) \cup \mathrm{FV}(u)$ and $\mathrm{FV}(t'u) = \mathrm{FV}(t') \cup \mathrm{FV}(u)$. By induction hypothesis, $\mathrm{FV}(t') \subseteq \mathrm{FV}(tu)$. therefore, $\mathrm{FV}(t'u) \subseteq \mathrm{FV}(tu)$.
   - Case $tu \rightarrow_\beta tu'$ since $u \rightarrow_\beta u'$. Similar to previous case.

2. Let $\sigma = \{y \mapsto v\}$ and $\sigma' = \{y \mapsto v'\}$. We proceed by induction on t.

- Case $t = y$. Then, $t\sigma = v$ and $t\sigma' = v'$. Thus, $t\sigma \to_\beta^* t\sigma'$.
- Case $t \in \mathcal{X} - \{y\}$. Then, $t\sigma = x = t\sigma'$. Thus, $t\sigma \to_\beta^* t\sigma'$.
- Case $t = \lambda xu$. By renaming, we can assume that $x \notin \{y\} \cup \mathrm{FV}(v)$. After property 1, $x \notin \mathrm{FV}(v')$. Hence, $t\sigma = \lambda x(u\sigma)$ and $t\sigma' = \lambda x(u\sigma')$. By induction hypothesis, $u\sigma \to_\beta u\sigma'$. Therefore, $t\sigma \to_\beta^* t\sigma'$.
- Case $t = ab$. Then, $t\sigma = (a\sigma)(b\sigma)$ and $t\sigma' = (a\sigma')(b\sigma')$. By induction hypothesis, $a\sigma \to_\beta^* a\sigma'$ and $b\sigma \to_\beta^* b\sigma'$. Therefore, $t\sigma \to_\beta^* (a\sigma')(b\sigma)$ and $(a\sigma')(b\sigma) \to_\beta^* (a\sigma')(b\sigma')$. Since $\to_\beta^*$ is transitive, $t\sigma \to_\beta^* t\sigma'$.

3. Let $\sigma = \{y \mapsto v\}$. We proceed by induction on the definition of $\to_\beta$.

- Case $(\lambda xt)u \to_\beta t\{x \mapsto u\}$. By renaming, we can assume that $x \notin \{y\} \cup \mathrm{FV}(v) \cup \mathrm{FV}(u)$. Hence, we have $((\lambda xt)u)\sigma = (\lambda x(t\sigma))(u\sigma)$ and $(t\{x \mapsto u\})\sigma = (t\sigma)\{x \mapsto u\sigma\}$ (can be proved by induction on t). Therefore, $((\lambda xt)u)\sigma \to_\beta (t\{x \mapsto u\})\sigma$.
- Case $\lambda xt \to_\beta \lambda xt'$ since $t \to_\beta t'$. By renaming, we can assume that $x \notin \{y\} \cup \mathrm{FV}(v)$. Hence, we have $(\lambda xt)\sigma = \lambda x(t\sigma)$ and $(\lambda xt')\sigma = \lambda x(t'\sigma)$. By induction hypothesis, $t\sigma \to_\beta t'\sigma$. Therefore, $(\lambda xt)\sigma \to_\beta (\lambda xt')\sigma$.
- Case $tu \to_\beta t'u$ since $t \to_\beta t'$. We have $(tu)\sigma = (t\sigma)(u\sigma)$ and $(t'u)\sigma = (t'\sigma)(u\sigma)$. By induction hypothesis, $t\sigma \to_\beta t'\sigma$. Therefore, $(tu)\sigma \to_\beta (t'u)\sigma$.
- Case $tu \to_\beta tu'$ since $u \to_\beta u'$. Similar to previous case.

4. We proceed by induction on the definition of $t \to_\beta u$, and by case on $t \to_\beta v$.

- Case $t = (\lambda xa)b$ and $u = a\{x \mapsto b\}$.
  - Case $v = u$. Then, it suffices to take $w = v = u$.
  - Case $v = (\lambda xa')b$ and $a \to_\beta a'$. Then, take $w = a'\{x \mapsto b\}$. We have $u \to_\beta w$ by property 3. And we have $v \to_\beta w$ by definition of $\to_\beta$.
  - Case $v = (\lambda xa)b'$ and $b \to_\beta b'$. Then, take $w = a\{x \mapsto b'\}$. We have $u \to_\beta^* w$ by property 2. And we have $v \to_\beta w$ by definition of $\to_\beta$.
- Case $t = \lambda xa$, $u = \lambda xa'$ and $a \to_\beta a'$. Then, $v = \lambda xc$ and $a \to_\beta c$. By induction hypothesis, there is d such that $a' \to_\beta^* d$ and $c \to_\beta^* d$. Therefore, by taking $w = \lambda xd$, we have $u \to_\beta^* w$ and $v \to_\beta^* w$.
- Case $t = ab$, $u = a'b$ and $a \to_\beta a'$.
  - Case $v = ac$ and $a \to_\beta c$. By induction hypothesis, there is d such that $a' \to_\beta^* d$ and $c \to_\beta^* d$. Therefore, by taking $w = db$, we have $u \to_\beta^* w$ and $v \to_\beta^* w$.
  - Case $v = ab'$ and $b \to_\beta b'$. Then, by taking $w = a'b'$, we have $u \to_\beta w$ and $v \to_\beta w$.
- Case $tu \to_\beta tu'$ since $u \to_\beta u'$. Similar to previous case.

Exercise 3 Define a 2-tapes Turing machine $(\Sigma, Q, q_i, q_f, \delta)$ computing the function $n \mapsto 2n$, where Σ is the finite alphabet used by the machine with at least the symbols $\{\square, 0, 1\}$, Q is the finite set of states of the machine, q_i the initial state, q_f the final state, and δ is a partial function from $Q \times \Sigma^2$ to $Q \times \Sigma^2 \times \{-1, 0, +1\}$. To do this, you are free to introduce in Σ symbols different from $\{\square, 0, 1\}$, and in Q states different from $\{q_i, q_f\}$. The machine starts in position 0 in state q_i with, on tape 1, $\square$ followed by n 1's and then 0's, and on tape 2, $\square$ followed by 0's. It must end in position 0 in state q_f with, on tape 2, $\square$ followed by $2n$ 1's and then 0's.

Proof. One possibility is to use a new symbol m to mark where we stopped and, for each 1 on tape 1, replace 1 by m on tape 1 and replace m on tape 2 by two 1's. We will also introduce new states as needed.

We first add an m in position 1 in tape 2 by the rules (x denotes the letter on tape 1, and y the letter on tape 2, where letters belong to $\Sigma = \{\square, 0, 1, m\}$):

- $(q_i, xy) \to (q_0, xy, 1)$
- $(q_0, xy) \to (q_1, xm, 0)$

We then parse tape 1 until a 0 or a 1 is reached. If we reach a 0, then we go back to position 0 and stop:

- $(q_1, 0y) \to (q_2, 0y, -1)$
- $(q_2, my) \to (q_2, my, -1)$
- $(q_2, \square y) \to (q_f, \square y, 0)$

If we reach a 1, then we replace it by m, go back to position 0:

- $(q_1, 1y) \to (q_3, my, -1)$
- $(q_3, my) \to (q_3, my, -1)$
- $(q_3, \square y) \to (q_4, \square y, 1)$

add two 1's at the end of tape 2, and go back to position 0 to start again on state q_1:

- $(q_4, x1) \to (q_4, x1, 1)$
- $(q_4, xm) \to (q_5, x1, 1)$
- $(q_5, xy) \to (q_6, x1, -1)$
- $(q_6, x1) \to (q_6, x1, -1)$
- $(q_6, x\square) \to (q_1, x\square, 1)$

Exercise 4 We consider a set $\mathcal{X}$ of variables, a set $\mathcal{F}$ of function symbols and a set $\mathcal{P}$ of predicate symbols. We assume that every (function or predicate) symbol f is equipped with an arity $\alpha_{\mathsf{f}} \in \mathbb{N}$, that is, in a term of the form $\mathsf{f}(t_1, \ldots, t_n)$, we always have $n = \alpha_{\mathsf{f}}$. A model is given by a set A and, for each function symbol f of arity n, a function $\mathsf{f}_A : A^n \to A$ and, for each predicate symbol P of arity n, a function $\mathsf{P}_A : A^n \to \mathsf{Bool}$ where $\mathsf{Bool} = \{\mathsf{true}, \mathsf{false}\}$. Then, given a finite valuation $\mu : \mathcal{X} \to A$, the interpretation of a formula ϕ, written $[\![\phi]\!]_\mu$, is defined as follows:

- $[\![x]\!]_\mu = \mu(x)$
- $[\![\mathsf{f}(t_1, \ldots, t_n)]\!]_\mu = \mathsf{f}_A([\![t_1]\!]_\mu, \ldots, [\![t_n]\!]_\mu)$
- $[\![\mathsf{P}(t_1, \ldots, t_n)]\!]_\mu = \mathsf{P}_A([\![t_1]\!]_\mu, \ldots, [\![t_n]\!]_\mu)$
- $[\![\bot]\!]_\mu = \mathsf{false}$
- $[\![\neg\phi]\!]_\mu = \mathsf{not}([\![\phi]\!]_\mu)$
- $[\![\phi \vee \psi]\!]_\mu = \mathsf{or}([\![\phi]\!]_\mu, [\![\psi]\!]_\mu)$
- $[\![\phi \wedge \psi]\!]_\mu = \mathsf{and}([\![\phi]\!]_\mu, [\![\psi]\!]_\mu)$
- $[\![\phi \Rightarrow \psi]\!]_\mu = \mathsf{impl}([\![\phi]\!]_\mu, [\![\psi]\!]_\mu)$
- $[\![\forall x\phi]\!]_\mu = \mathsf{forall}(\{[\![\phi]\!]_{\mu \cup \{x,a\}} \mid a \in A\})$ if $x \notin \mathrm{dom}(\mu)$
- $[\![\exists x\phi]\!]_\mu = \mathsf{exists}(\{[\![\phi]\!]_{\mu \cup \{x,a\}} \mid a \in A\})$ if $x \notin \mathrm{dom}(\mu)$

where $\mathrm{dom}(\mu)$ is the set of variables on which μ is defined, the boolean functions not, or, ... are defined as usual, and $\mathsf{forall}, \mathsf{exists} : \mathcal{P}(\mathsf{Bool}) \to \mathsf{Bool}$ are defined as follows:

- $\mathsf{forall}(S) = \mathsf{true}$ iff $\mathsf{false} \notin S$
- $\mathsf{exists}(S) = \mathsf{true}$ iff $\mathsf{true} \in S$

The universal closure of a formula ϕ with free variables $x_1, \ldots, x_n$ is $\overline{\forall}\phi = \forall x_1 \ldots \forall x_n \phi$. A formula ϕ is *valid* if, in every model A, $[\![\overline{\forall}\phi]\!] = \mathsf{true}$.

Let the provability relation $\vdash$ be the smallest relation on pairs (Γ, ϕ) where Γ is a finite set of formulas (the assumptions) and ϕ a formula, such that:

$$(\text{axiom}) \quad \frac{\phi \in \Gamma}{\Gamma \vdash \phi}$$

$$(\bot\text{-elim}) \quad \frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}$$

$$(\Rightarrow\text{-intro}) \quad \frac{\Gamma \cup \{\phi\} \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}$$

$$(\Rightarrow\text{-elim})\quad \frac{\Gamma \vdash \phi \Rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$(\wedge\text{-intro})\quad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}$$

$$(\wedge\text{-elim-left})\quad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}$$

$$(\wedge\text{-elim-right})\quad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}$$

$$(\vee\text{-intro-left})\quad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}$$

$$(\vee\text{-intro-right})\quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}$$

$$(\vee\text{-elim})\quad \frac{\Gamma \vdash \phi \vee \psi \quad \Gamma \cup \{\phi\} \vdash \chi \quad \Gamma \cup \{\psi\} \vdash \chi}{\Gamma \vdash \chi}$$

$$(\forall\text{-intro})\quad \frac{\Gamma \vdash \phi \quad x \notin \mathrm{FV}(\Gamma)}{\Gamma \vdash \forall x \phi}$$

$$(\forall\text{-elim})\quad \frac{\Gamma \vdash \forall x \phi}{\Gamma \vdash \phi\{x \mapsto t\}}$$

$$(\exists\text{-intro})\quad \frac{\Gamma \vdash \phi\{x \mapsto t\}}{\Gamma \vdash \exists x \phi}$$

$$(\exists\text{-elim})\quad \frac{\Gamma \vdash \exists x \phi \quad \Gamma \cup \{\phi\} \vdash \chi \quad x \notin \mathrm{FV}(\Gamma) \cup \mathrm{FV}(\chi)}{\Gamma \vdash \chi}$$

$$(\mathrm{EM})\quad \Gamma \vdash \phi \vee \neg\phi$$

Prove that the provability relation is correct, that is, in every model A, if $\Gamma \vdash \phi$ and $\Gamma = \{\phi_1, \ldots, \phi_n\}$, then $\phi_1 \wedge \ldots \wedge \phi_n \Rightarrow \phi$ is valid.

Proof. We proceed by induction on the definition of $\vdash$. Let $\Gamma = \{\phi_1, \ldots, \phi_n\}$. In the following, we identity Γ and the formula $\phi_1 \wedge \ldots \wedge \phi_n$. Let A be a model and μ a valuation such that $\mathrm{dom}(\mu) \subseteq \mathrm{FV}(\Gamma)$ and $[\![\Gamma]\!]_\mu = \mathsf{true}$.

($\wedge$-intro) We have $[\![\phi \wedge \psi]\!] = \mathsf{and}([\![\phi]\!]_\mu, [\![\psi]\!]_\mu)$. By induction hypothesis, $[\![\phi]\!]_\mu = \mathsf{true}$ and $[\![\psi]\!]_\mu = \mathsf{true}$. Therefore, $[\![\phi \wedge \psi]\!] = \mathsf{true}$.

($\wedge$-elim-left) By induction hypothesis, we have $[\![\phi \wedge \psi]\!]_\mu = \mathsf{and}([\![\phi]\!]_\mu, [\![\psi]\!]_\mu) = \mathsf{true}$. Therefore, $[\![\phi]\!]_\mu = \mathsf{true}$.

($\wedge$-elim-right) Similar.

(∀-intro) We have $[\![\forall x\phi]\!]_\mu = \mathsf{forall}(\{[\![\phi]\!]_{\mu\cup\{x,a\}} \mid a \in A\})$. But, for all $a \in A$, by induction hypothesis, we have $[\![\phi]\!]_{\mu\cup\{x,a\}} = \mathsf{true}$. Therefore, $[\![\forall x\phi]\!]_\mu = \mathsf{true}$.

(∀-elim) By induction hypothesis, we have $[\![\forall x\phi]\!] = \mathsf{forall}(\{[\![\phi]\!]_{\mu\cup\{x,a\}} \mid a \in A\}) = \mathsf{true}$. Therefore, by definition of forall, we have $[\![\phi\{x \mapsto t\}]\!]_\mu = \mathsf{true}$ since $[\![\phi\{x \mapsto t\}]\!]_\mu = [\![\phi]\!]_{\mu\cup\{x\mapsto a\}}$ where $a = [\![t]\!]_\mu$ (can be proved by induction on ϕ).

...