Master Parisien de Recherche en Informatique
École normale supérieure

Année scolaire 2009/2010

Cours M.2-6
« Interprétation abstraite: applications à la vérification et à l'analyse statique »

Corrigé de l'examen partiel

Patrick Cousot

20 novembre 2009

Course and personal notes are the only allowed documents. It will not be answered to any question during the exam. If a question is ambiguous, imprecise or incorrect, it is part of the question to solve the ambiguity, imprecision or incorrectness by indicating all required hypotheses together with the solution, if any.

We describe the syntax of grammars using the following meta-grammar (that is grammar of grammars).

$$
\begin{array}{rcll}
\mathbb{T} & & & \text{terminals } T \\
\mathbb{N} & & & \text{nonterminals } N \\
\mathbb{V} & \triangleq & \mathbb{T} \cup \mathbb{N} & \text{vocabulary } (\mathbb{T} \cap \mathbb{N} = \emptyset) \\
G & ::= & P\ G \quad | \quad P & \text{grammar} \\
P & ::= & N \text{ `::='} \ ARS & \text{production} \\
ARS & ::= & RS \text{ `|'} \ ARS \quad | \quad RS & \text{alternative right sides} \\
RS & ::= & S\ RS \quad | \quad S & \text{right sides} \\
S & ::= & N \quad | \quad T \quad | \quad \text{`}\varepsilon\text{'} & \text{symbols}
\end{array}
$$

This meta-grammar has the meta-symbols ::=, |, ε, the meta-terminals {'::=', '|', 'ε'} $\cup\ \mathbb{V}$ such that {'::='; '|', 'ε'} $\notin \mathbb{V}$ and the meta-nonterminals {G, P, ARS, RS, S, N, T} $\notin \mathbb{V}$. We assume that all productions of the grammar with the same left side nonterminal have their right sides grouped, with the alternative right sides separated by |. For example

$$\begin{array}{lcl} X & ::= & YX \\ & | & \varepsilon \\ Y & ::= & a \\ & | & b \end{array}$$

Question 1

Provide a structural definition of the transition system of a grammar (by induction on the meta-grammar).

Answer to question 5

The structural definition of the transition system of a grammar is

$$\begin{array}{rcl} \tau[\![PG]\!] & = & \tau[\![P]\!] \ \cup \ \tau[\![G]\!] \\ \tau[\![N\text{'::='}ARS]\!] & = & \{\langle pNq,\ prq\rangle \mid p, q \in \mathbb{V}[\![G]\!]^\star \wedge r \in \mathbb{A}[\![ARS]\!]\} \\ \mathbb{A}[\![RS\ \text{'|'}ARS]\!] & \triangleq & \mathbb{A}[\![RS]\!] \ \cup \ \mathbb{A}[\![ARS]\!] \\ \mathbb{A}[\![SRS]\!] & \triangleq & \mathbb{A}[\![S]\!] \cdot \mathbb{A}[\![RS]\!] \\ \mathbb{A}[\![N]\!] & \triangleq & \{N\} \\ \mathbb{A}[\![T]\!] & \triangleq & \{T\} \\ \mathbb{A}[\![\text{'}\varepsilon\text{'}]\!] & \triangleq & \{\epsilon\} \end{array} \tag{1}$$

Question 2

Prove that the correctness of the structural definition of the transition system of a grammar (that is the equivalence of the definitions in questions 4 and 5).

Answer to question 6

In equation (1), we have defined:

$$\begin{array}{lrcl} & \tau[\![G]\!] & \triangleq & \alpha(\mathbb{P}[\![G]\!]) \\ \text{where} & \alpha(X) & \triangleq & \{\langle pNq,\ prq\rangle \mid p, q \in \mathbb{V}[\![G]\!]^\star \wedge \langle N,\ r\rangle \in X\} \end{array}$$

Let $\tau'[\![G]\!]$ satisfying eq. (2). We prove that $\tau[\![G]\!] = \tau'[\![G]\!]$ by structural induction on the metasyntax of G.

— $\tau[\![PG]\!]$

$$\begin{aligned}
&= \alpha(\mathbb{P}[\![PG]\!]) && \wr\text{def. } \tau[\![G]\!]\wr\\
&= \alpha(\mathbb{P}[\![P]\!] \cup \mathbb{P}[\![G]\!]) && \wr\text{def. } \mathbb{P}[\![P]\!]\wr\\
&= \alpha(\mathbb{P}[\![P]\!]) \cup \alpha(\mathbb{P}[\![G]\!]) && \wr\alpha \text{ preserves joins}\wr\\
&= \tau[\![P]\!] \cup \tau[\![G]\!] && \wr\text{def. } \tau[\![G]\!]\wr\\
&= \tau'[\![P]\!] \cup \tau'[\![G]\!] && \wr\text{induction hyp.}\wr\\
&= \tau'[\![PG]\!] && \wr\text{def. eq. (2) of } \tau'[\![G]\!]\wr
\end{aligned}$$

— $\tau[\![N\text{'::='}ARS]\!]$

$$\begin{aligned}
&= \alpha(\mathbb{P}[\![N\text{'::='}ARS]\!]) && \wr\text{def. } \tau[\![G]\!]\wr\\
&= \alpha(\{\langle N,\ r\rangle \mid r \in \mathbb{A}[\![ARS]\!]\}) && \wr\text{def. } \mathbb{P}[\![P]\!]\wr\\
&= \{\langle pNq,\ prq\rangle \mid p, q \in \mathbb{V}[\![G]\!]^\star \wedge r \in \mathbb{A}[\![ARS]\!]\} && \wr\text{def. } \alpha\wr\\
&= \tau'[\![N\text{'::='}ARS]\!] && \wr\text{def. eq. (2) of } \tau'[\![P]\!]\wr
\end{aligned}$$

— $\mathbb{A}[\![RS \text{ '|' } ARS]\!]$

$$\begin{aligned}
&= \{\mathbb{R}[\![RS]\!]\} \quad\cup\quad \mathbb{A}[\![ARS]\!] && \wr\text{def. } \mathbb{A}[\![ARS]\!]\wr\\
&= \mathbb{A}[\![RS]\!] \quad\cup\quad \mathbb{A}[\![ARS]\!] && \wr\text{def. } \mathbb{A}[\![RS]\!]\wr
\end{aligned}$$

— $\mathbb{A}[\![S\ RS]\!]$

$$\begin{aligned}
&= \{\mathbb{R}[\![S\ RS]\!]\} && \wr\text{def. } \mathbb{A}[\![RS]\!]\wr\\
&= \{\mathbb{R}[\![S]\!] \cdot \mathbb{R}[\![RS]\!]\} && \wr\text{def. } \mathbb{R}[\![RS]\!]\wr\\
&= \{\mathbb{R}[\![S]\!]\} \cdot \{\mathbb{R}[\![RS]\!]\} && \wr\text{def. } \cdot\wr\\
&= \mathbb{A}[\![S]\!] \cdot \mathbb{A}[\![RS]\!] && \wr\text{def. } \mathbb{A}[\![S]\!] \ \&\ \mathbb{A}[\![RS]\!]\wr
\end{aligned}$$

— $\mathbb{A}[\![N]\!] \quad=\quad \{\mathbb{R}[\![N]\!]\} \quad=\quad \{N\}$

— $\mathbb{A}[\![T]\!] \quad=\quad \{\mathbb{R}[\![T]\!]\} \quad=\quad \{T\}$

— $\mathbb{A}[\![\text{'}\varepsilon\text{'}]\!] \quad=\quad \{\mathbb{R}[\![\text{'}\varepsilon\text{'}]\!]\} \quad=\quad \{\epsilon\}$

Question 3

Let us define the *reflexive transitive closure* $r^\star$ of a relation $r \in \wp(S \times S)$ on a set S as $r^\star \triangleq \bigcup_{n\geqslant 0} r^n$ where the *powers* r^n of r are $r^0 \triangleq \{\langle x,\ x\rangle \mid x \in S\} \triangleq \mathbb{1}_S$ (identity relation), $r^{n+1} = r^n \circ r = r \circ r^n$, and the composition of relations is $r \circ r' \triangleq \{\langle x,\ x''\rangle \mid \exists x' \in S : \langle x,\ x'\rangle \in r \wedge \langle x',\ x''\rangle \in r'\}$. Prove that $r^\star =$

$\mathbf{lfp}_{\emptyset}^{\subseteq}\ \lambda X \cdot \mathbb{1}_S \cup r \circ X = \mathbf{lfp}_{\emptyset}^{\subseteq}\ \lambda X \cdot \mathbb{1}_S \cup X \circ r$ (where $\mathbf{lfp}_a^{\leqslant} f$ is the $\leqslant$-least fixpoint of f which is $\leqslant$-greater than or equal to a, if any).

Answer to question 7

Theorem 1

$$r^\star \quad = \quad \boldsymbol{lfp}^{\subseteq}\ \lambda X \cdot \mathbb{1}_S \cup X \circ r$$

Proof — $\langle \wp(S \times S), \subseteq, \emptyset, S, \cup, \cap \rangle$ is a complete lattice and $\lambda X \cdot \mathbb{1}_S \cup X \circ r$ is increasing since

$$
\begin{array}{ll}
\quad X \subseteq Y & \wr \text{hypothesis} \wr \\
\Rightarrow X \circ r \subseteq Y \circ r & \wr \text{def. relation composition } \circ \wr \\
\Rightarrow \mathbb{1}_S \cup X \circ r \subseteq \mathbb{1}_S \cup Y \circ r & \wr \text{def. lub} \wr
\end{array}
$$

$\lambda X \cdot r \circ (\mathbb{1}_S \cup X)$ is increasing since

$$
\begin{array}{ll}
\quad X \subseteq Y & \wr \text{hypothesis} \wr \\
\Rightarrow (\mathbb{1}_S \cup X) \subseteq (\mathbb{1}_S \cup Y) & \wr \text{def. lub} \wr \\
\Rightarrow r \circ (\mathbb{1}_S \cup X) \subseteq r \circ (\mathbb{1}_S \cup Y) & \wr \text{def. relation composition } \circ \wr
\end{array}
$$

— The existence of the fixpoints follows from Tarski's fixpoint theorem.

— We have $r^\star = \bigcup_{n \in \mathbb{N}} r^n = r^0 \cup \bigcup_{n>0} r^n = r^0 \cup \bigcup_{n \geq 0} r^{n+1} = r^0 \cup \bigcup_{n \geq 0} (r \circ r^n)$ $= r^0 \cup r \circ (\bigcup_{n \geq 0} r^n) = \mathbb{1}_S \cup r \circ r^\star$ so that $r^\star$ is a fixpoint of $\lambda X \cdot \mathbb{1}_S \cup X$. Let R be another fixpoint that is $R = \mathbb{1}_S \cup X \circ R$. We have $r^0 = \mathbb{1}_S \subseteq = \mathbb{1}_S \cup X \circ R = R$. Assume by induction hypothesis that $r^n \subseteq R$ then $r^{n+1} = r \circ r^n \subseteq r \circ R \subseteq \mathbb{1}_S \cup X \circ R = R$. By recurrence, $\forall n : r^n \subseteq R$ proving $r^\star = \bigcup_{n \in \mathbb{N}} r^n \subseteq R$ to be the least fixpoint. ∎

Question 4

The derivation semantics of a grammar is the reflexive transitive closure $\tau[\![G]\!]^\star$ of its transition semantics $\tau[\![G]\!]$ defined in questions 4 and 5. Let us define the $\subseteq$-increasing transformer:

$$B[\![ARS]\!] \quad \in \quad \wp(\mathbb{V}^\star \times \mathbb{V}^\star) \xrightarrow{\nearrow} \wp(\mathbb{V}^\star)$$

as follows:

$$
\begin{aligned}
B[\![RS \mid ARS]\!]r &\triangleq B[\![RS]\!]r \;\cup\; B[\![ARS]\!]r && (2)\\
B[\![SRS]\!]r &\triangleq B[\![S]\!]r \cdot B[\![RS]\!]r && (3)\\
B[\![N]\!]r &\triangleq \{p \mid \langle N,\, p\rangle \in r\} && (4)\\
B[\![T]\!]r &\triangleq \{T\} && (5)\\
B[\![\varepsilon]\!]r &\triangleq \{\varepsilon\} && (6)
\end{aligned}
$$

where $X \cdot Y = \{pq \mid p \in X \wedge q \in Y\}$ is the concatenation of sets of protosentences and ε is the empty protosentence.

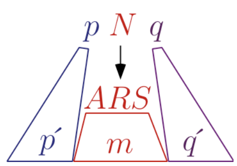
Let us define

$$B[\![G]\!] \quad \in \quad \wp(\mathbb{V}^\star \times \mathbb{V}^\star) \xrightarrow{\nearrow} \wp(\mathbb{V}^\star \times \mathbb{V}^\star)$$

as follows:

$$
\begin{aligned}
B[\![PG]\!]r &\triangleq B[\![P]\!]r \cup B[\![G]\!]r && (7)\\
B[\![N ::= ARS]\!]r &\triangleq \mathsf{I}_{\mathbb{V}^\star} \cup \{\langle pNq,\, p'mq'\rangle \mid \langle p,\, p'\rangle \in r \wedge && (8)\\
&\qquad\qquad m \in B[\![ARS]\!]r \wedge \langle q,\, q'\rangle \in r\}
\end{aligned}
$$

which can be illustrated as follows



Prove that $\mathbf{lfp}^{\subseteq}_{\emptyset}\, B[\![G]\!] = \tau[\![G]\!]^\star$.

Answer to question 8

Lemma 2 (Derivation Extension Lemma) *If* $\langle p, q\rangle \in \tau[\![G]\!]^\star$ *and* $\langle r, s\rangle \in \tau[\![G]\!]^\star$ *then* $\langle pr,\, qs\rangle \in \tau[\![G]\!]^\star$. □

Proof — Let us first prove that

if $\langle p,\, q\rangle \in \tau[\![G]\!]$ then $\langle rp,\, rq\rangle \in \tau[\![G]\!]$ and $\langle ps,\, qs\rangle \in \tau[\![G]\!]$. (9)

Indeed

$\langle p,\ q\rangle \in \tau[\![G]\!]$

$\Rightarrow\ \exists p_1, p_2, N, m : p = p_1 N p_2 \land q = p_1 m p_2 \land \langle N,\ m\rangle \in \mathbb{P}[\![G]\!]$ $\wr$def. $\tau[\![G]\!]\int$

$\Rightarrow\ \exists p_1, p_2, N, m : rp = rp_1 N p_2 \land rq = rp_1 m p_2 \land \langle N,\ m\rangle \in \mathbb{P}[\![G]\!]$ $\wr$def. string equality$\int$

$\Rightarrow\ \langle rp,\ rq\rangle \in \tau[\![G]\!]$ $\wr$def. $\tau[\![G]\!]\int$

The proof is symmetric in the second case.

— Let us now prove that

$$\text{if } \langle p,\ q\rangle \in \tau[\![G]\!]^\star \text{ then } \langle rp,\ rq\rangle \in \tau[\![G]\!]^\star \text{ and } \langle ps,\ qs\rangle \in \tau[\![G]\!]^\star \qquad (10)$$

The proof is by recurrence on $n \geq 0$ for $\tau[\![G]\!]^n$.

- For $n = 0$, $\langle p,\ q\rangle \in \tau[\![G]\!]^0 = \mathrm{I}_{\mathbb{V}^\star}$ so $p = q$ hence $rp = rq$ proving $\langle rp,\ rq\rangle \in \tau[\![G]\!]^0$.
- For $n+1$, if $\langle p,\ q\rangle \in \tau[\![G]\!]^{n+1}$ then $\exists p' : \langle p,\ p'\rangle \in \tau[\![G]\!]^n$ and $\langle p',\ q\rangle \in \tau[\![G]\!]$. So $\langle rp,\ rp'\rangle \in \tau[\![G]\!]^n$ by induction hypothesis and $\langle rp',\ rq\rangle \in \tau[\![G]\!]$ by the previous lemma (10) so $\langle rp,\ rq\rangle \in \tau[\![G]\!]^{n+1}$ by composition.

If $\langle p,\ q\rangle \in \tau[\![G]\!]^\star$ then $\exists n : \langle p,\ q\rangle \in \tau[\![G]\!]^n$ so $\langle rp,\ rq\rangle \in \tau[\![G]\!]^n \subseteq \tau[\![G]\!]^\star$.
The proof is symmetric in the second case.

— Finally, if $\langle p,\ q\rangle \in \tau[\![G]\!]^\star$ and $\langle r,\ s\rangle \in \tau[\![G]\!]^\star$ then $\langle pr,\ qr\rangle \in \tau[\![G]\!]^\star$ and $\langle qr,\ qs\rangle \in \tau[\![G]\!]^\star$ by the previous lemma (11) so that $\langle pr,\ qs\rangle \in \tau[\![G]\!]^\star$ by composition. ■

Lemma 3 (Separate Derivation Lemma) *For all $n \in \mathbb{N}$, $\langle pq,\ m\rangle \in \tau[\![G]\!]^n$ if and only if $\exists p', q' \in \mathbb{V}^\star : \exists n_1, n_2 \in \mathbb{N} : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \land \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \land n = n_1 + n_2 \land m = p'q'$* □

Proof By recurrence on n. — For $n = 0$, we have:

$\langle pq,\ m\rangle \in \tau[\![G]\!]^0$

$\Leftrightarrow\ m = pq$ $\wr$def. $\tau[\![G]\!]^0 = \mathrm{I}_{\mathbb{V}^\star}\int$

$\Leftrightarrow\ \exists p', q' : p = p' \land q = q' \land m = p'q'$ $\wr$def. string equality$\int$

$\Leftrightarrow\ \exists p', q' \in \mathbb{V}^\star : \exists n_1, n_2 \in \mathbb{N} : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \land \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \land 0 = n_1 + n_2 \land m = p'q'$ $\wr$since $n_1, n_2 \in \mathbb{N}$ and $n_1 + n_2 = 0$ implies $n_1 = n_2 = 0\int$

— For $n+1$, we have:

$\langle pq,\ m\rangle \in \tau[\![G]\!]^{n+1}$

$\Leftrightarrow$ $\exists m' : \langle pq,\ m'\rangle \in \tau[\![G]\!]^{n} \wedge \langle m',\ m\rangle \in \tau[\![G]\!]$ $\wr$def. $\tau[\![G]\!]^{n+1} = \tau[\![G]\!]^{n} \circ \tau[\![G]\!]$ and $\circ\wr$

$\Leftrightarrow$ $\exists p', q', n_1, n_2 : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \wedge n = n_1 + n_2 \wedge m' = p'q' \wedge \langle p'q',\ m\rangle \in \tau[\![G]\!]$ $\wr$by ind. hyp.$\wr$

$\Leftrightarrow$ $\exists p', q', n_1, n_2, N, r : \langle p, p'\rangle \in \tau[\![G]\!]^{n_1} \wedge \langle q, q'\rangle \in \tau[\![G]\!]^{n_2} \wedge n = n_1 + n_2 \wedge m' = p'q' \wedge [(\exists p_1, p_2 : p' = p_1 N p_2 \wedge m = p_1 r p_2 q') \vee (\exists q_1, q_2 : q' = q_1 N q_2 \wedge m = p' q_1 r q_2)] \wedge \langle N,\ r\rangle \in \mathbb{P}[\![G]\!]$ $\wr$by def. $\tau[\![G]\!]$ and string equality$\wr$

$\Leftrightarrow$ $\exists p', q', n_1, n_2 : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \wedge n = n_1 + n_2 \wedge m' = p'q' \wedge [(\exists p'' : \langle p',\ p''\rangle \in \tau[\![G]\!] \wedge m = p''q') \vee (\exists q'' : \langle q',\ q''\rangle \in \tau[\![G]\!] \wedge m = p'q'')]$ $\wr$by def. $\tau[\![G]\!]\wr$

$\Leftrightarrow$ $[\exists p'', q', n_1, n_2 : \langle p,\ p''\rangle \in \tau[\![G]\!]^{n_1+1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \wedge n + 1 = n_1 + n_2 + 1 \wedge m' = p''q'] \vee [\exists p', q'', n_1, n_2 : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \wedge \langle q,\ q''\rangle \in \tau[\![G]\!]^{n_2+1} \wedge n + 1 = n_1 + n_2 + 1 \wedge m' = p'q'']$ $\wr$def. $\tau[\![G]\!]^{n+1} = \tau[\![G]\!]^{n} \circ \tau[\![G]\!]$ and $\circ\wr$

$\Leftrightarrow$ $\exists p', q' \in \mathbb{V}^\star : \exists k_1, k_2 \in \mathbb{N} : \langle p,\ p'\rangle \in \tau[\![G]\!]^{k_1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{k_2} \wedge n + 1 = k_1 + k_2 \wedge m = p'q'$ $\wr$choosing either $k_1 = n_1 + 1$, $k_2 = n_2$ with $p' = p''$ or $k_1 = n_1$, $k_2 = n_2 + 1$ with $q' = q''\wr$ ■

Corollary 4 *If $r^n = \bigcup_{k=0}^{n} \tau[\![G]\!]^k$ then $\langle pq,\ m\rangle \in \tau[\![G]\!]^\star$ implies $\exists p', q' : \langle p,\ p'\rangle \in r^n \wedge \langle q,\ q'\rangle \in r^n \wedge m = p'q'$.* □

Proof

$\langle pq,\ m\rangle \in r^n$

$\Leftrightarrow$ $\exists k \le n : \langle pq,\ m\rangle \in \tau[\![G]\!]^k$ $\wr$since $r^n = \bigcup_{k=0}^{n} \tau[\![G]\!]^k\ \wr$

$\Rightarrow$ $\exists p', q', k_1 \le n, k_2 \le n : \langle p,\ p'\rangle \in \tau[\![G]\!]^{k_1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{k_2} \wedge m = p'q'$ $\wr$by the separate derivation lemma 3$\wr$

$\Rightarrow$ $\exists p', q' : \langle p,\ p'\rangle \in r^n \wedge \langle q,\ q'\rangle \in r^n \wedge m = p'q'$ $\wr$since $r^n = \bigcup_{k=0}^{n} \tau[\![G]\!]^k\ \wr$ ■

Corollary 5 *$\langle pq,\ m\rangle \in \tau[\![G]\!]^\star$ if and only if $\exists p', q' : \langle p,\ p'\rangle \in \tau[\![G]\!]^\star \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^\star \wedge m = p'q'$.* □

PROOF

$\langle pq,\ m\rangle \in \tau[\![G]\!]^\star$

$\Leftrightarrow\ \exists n \in \mathbb{N} : \langle pq,\ m\rangle \in \tau[\![G]\!]^n$ $\quad$ ≀since $\tau[\![G]\!]^\star = \bigcup_{n\in\mathbb{N}} \tau[\![G]\!]^n$∫

$\Leftrightarrow\ \exists p', q', n_1, n_2 : \langle p,\ p'\rangle \in \tau[\![G]\!]^{n_1} \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^{n_2} \wedge m = p'q'$ $\quad$ ≀by the separate derivation lemma 3∫

$\Leftrightarrow\ \exists p', q' : \langle p,\ p'\rangle \in \tau[\![G]\!]^\star \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^\star \wedge m = p'q'$ $\quad$ ≀since $\tau[\![G]\!]^\star = \bigcup_{n\in\mathbb{N}} \tau[\![G]\!]^n$∫ ■

Theorem 6 (Fixpoint Grammar Derivation Semantics) $\tau[\![G]\!]^\star = \boldsymbol{lfp}^{\subseteq} B[\![G]\!]$ *where* $B[\![G]\!]$ *is defined in definitions (8) and (9).* □

PROOF —— We first prove that $B[\![G]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$ so that by Tarski's least fixpoint, we conclude that $\mathbf{lfp}^{\subseteq} B[\![G]\!] \subseteq \tau[\![G]\!]^\star$;

—— Then we prove that $\tau[\![G]\!]^\star \subseteq \mathbf{lfp}^{\subseteq} B[\![G]\!]$ and conclude by antisymmetry.

—— The first part of the proof consists in proving that $B[\![G]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$.

— First, we show that

$$\mathbb{A}[\![S]\!] \times B[\![S]\!](\tau[\![G]\!]^\star) \quad \subseteq \quad \tau[\![G]\!]^\star \tag{11}$$

The proof is by case analysis.

- If $S = \varepsilon$ then $B[\![\varepsilon]\!](\tau[\![G]\!]^\star) = \{\varepsilon\}$ by (7) and $\langle \varepsilon,\ \varepsilon\rangle \in \tau[\![G]\!]^\star$ by reflexivity;
- If $S = T$ then $B[\![T]\!](\tau[\![G]\!]^\star) = \{T\}$ by (6) and $\langle T,\ T\rangle \in \tau[\![G]\!]^\star$ by reflexivity;
- If $S = N$ then we have $\langle N, p\rangle \in \tau[\![G]\!]^\star$ by def. (5) of $B[\![N]\!](\tau[\![G]\!]^\star) \triangleq \{p \mid \langle N, p\rangle \in \tau[\![G]\!]^\star\}$.

— Second, we show that

$$\mathbb{A}[\![RS]\!] \times B[\![RS]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star \tag{12}$$

The proof is by structural induction on RS.

- The base case $RS = S$ has been already handled by the previous lemma (12);

- Otherwise $RS = SRS'$, in which case by (2) and (4), $\mathbb{A}[\![RS]\!] \times B[\![RS]\!](\tau[\![G]\!]^\star) = (\mathbb{A}[\![S]\!] \cdot \mathbb{A}[\![RS']\!]) \times (B[\![S]\!](\tau[\![G]\!]^\star) \cdot B[\![RS']\!](\tau[\![G]\!]^\star))$.

  We have $\mathbb{A}[\![S]\!] \times B[\![S]\!](\tau[\![G]\!]^\star) \subseteq (\tau[\![G]\!]^\star$ by the previous lemma (12) and $\mathbb{A}[\![RS']\!] \times B[\![RS']\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$ by induction hypothesis. It follows that $\mathbb{A}[\![RS]\!] \times B[\![RS]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$ by the derivation extension lemma 2.

— Third, we show that for any production $P = N ::= RS_1 \mid \ldots \mid RS_\ell$ (with $\ell \geq 1$) of the grammar G, we have:

$$\{N\} \times B[\![RS_i]\!](\tau[\![G]\!]^\star) \quad \subseteq \quad \tau[\![G]\!]^\star \tag{13}$$

Indeed, the definition (2) of $\tau[\![P]\!]$ when $p = q = \varepsilon$ implies that

$$\{N\} \times \mathbb{A}[\![RS_1 \mid \ldots \mid RS_\ell]\!] \quad \subseteq \quad \tau[\![P]\!] \quad \subseteq \quad \tau[\![G]\!]^\star$$

By definition (2) of $\mathbb{A}[\![RS_1 \mid \ldots \mid RS_\ell]\!] = \bigcup_{i=1}^{\ell} \mathbb{A}[\![RS_i]\!]$, we have

$$\{N\} \times \mathbb{A}[\![RS_i]\!] \quad \subseteq \quad \tau[\![G]\!]^\star$$

Moreover, by the previous lemma (13), $\mathbb{A}[\![RS_i]\!] \times B[\![RS_i]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$, hence by composition:

$$\{N\} \times B[\![RS_i]\!](\tau[\![G]\!]^\star) \quad \subseteq \quad \tau[\![G]\!]^\star \circ \tau[\![G]\!]^\star \quad \subseteq \quad \tau[\![G]\!]^\star$$

— Fourth, we show that for any production $P = N ::= ARS$ of the grammar G, we have:

$$\{N\} \times B[\![ARS]\!](\tau[\![G]\!]^\star) \quad \subseteq \quad \tau[\![G]\!]^\star \tag{14}$$

We have $ARS = RS_1 \mid \ldots \mid RS_\ell$ where $\ell \geq 1$. The definition (3) of $B[\![ARS]\!]$ implies that $B[\![ARS]\!] = \bigcup_{i=0}^{\ell} B[\![RS_i]\!]$. By the previous lemma (14), $\{N\} \times B[\![ARS]\!] = \{N\} \times \bigcup_{i=0}^{\ell} B[\![RS_i]\!](\tau[\![G]\!]^\star) = \bigcup_{i=0}^{\ell} \{N\} \times B[\![RS_i]\!](\tau[\![G]\!]^\star) \subseteq \bigcup_{i=0}^{\ell} \tau[\![G]\!]^\star = \tau[\![G]\!]^\star$.

— Fifth, we show that

$$B[\![N ::= ARS]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star \tag{15}$$

- By reflexivity, $\mathrm{I}_{\mathbb{V}^\star} \subseteq \tau[\![G]\!]^\star$;

– By the previous lemma (15), $m \in B[\![ARS]\!](\tau[\![G]\!]^\star)$ implies $\langle N,\ m\rangle \in \tau[\![G]\!]^\star$ so

$$\begin{aligned} & \{\langle pNq,\ p'mq'\rangle \mid \langle p,\ p'\rangle \in \tau[\![G]\!]^\star \wedge m \in B[\![ARS]\!](\tau[\![G]\!]^\star) \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^\star\} \\ \subseteq\ & \{\langle pNq,\ p'mq'\rangle \mid \langle p,\ p'\rangle \in \tau[\![G]\!]^\star \wedge \langle N,\ m\rangle \in \tau[\![G]\!]^\star \wedge \langle q,\ q'\rangle \in \tau[\![G]\!]^\star\} \\ \subseteq\ & \tau[\![G]\!]^\star \qquad \text{≀by the separate derivation corollary } \mathbf{5}\text{≀}; \end{aligned}$$

– By def. (9) of $B[\![N ::= ARS]\!](\tau[\![G]\!]^\star)$, we conclude that

$$B[\![N ::= ARS]\!](\tau[\![G]\!]^\star) \quad \subseteq \quad \tau[\![G]\!]^\star\ .$$

— Sixth and finally, we show that for any grammar $G = P_1 \dots P_\ell$ (where $\ell \geq 1$), we have $B[\![G]\!](\tau[\![G]\!]^\star) \subseteq \tau[\![G]\!]^\star$

Indeed, $G = P_1 \dots P_\ell$ with $\ell \geq 1$ and, by def. (8) and (9) of $B[\![G]\!]$, $B[\![G]\!](\tau[\![G]\!]^\star) = \bigcup_{i=1}^{\ell} B[\![G]\!](\tau[\![P_i]\!]^\star) \subseteq \bigcup_{i=1}^{\ell} \tau[\![P_i]\!]^\star = \tau[\![P_i]\!]^\star$ by the previous lemma (16).

—— The second part of the proof consists in proving that $\tau[\![G]\!]^\star \subseteq \mathbf{lfp}^{\subseteq}\, B[\![G]\!]$.

In the following we let $r^n = \bigcup_{k=0}^{n} \tau[\![G]\!]^k$.

— First, we show that

$$\langle \mathbb{R}[\![S]\!],\ m\rangle \in r^n \Rightarrow m \in B[\![S]\!]r^n \tag{16}$$

The proof is by case analysis.

– If $S = N$ then $\mathbb{R}[\![N]\!] \triangleq N$ so $\langle N,\ m\rangle \in r^n$ implies $m \in \{p \mid \langle N,\ p\rangle \in r\} = B[\![S]\!]r^n$;

– If $S = T$ then $\mathbb{R}[\![T]\!] \triangleq T$ so $\langle T,\ m\rangle \in r^n$ implies $\langle T,\ m\rangle \in \tau[\![G]\!]^0$ so $T = m$ since $\langle T,\ m\rangle \notin \tau[\![G]\!]$ by def. of $\tau[\![G]\!]$ so $\langle T,\ m\rangle\ /\tau[\![G]\!]^n$ when $n > 0$. It follows that $m = T \in \{T\} \triangleq B[\![T]\!]r$.

– If $S = \varepsilon$ then $\mathbb{R}[\![\varepsilon]\!] \triangleq \varepsilon$ so similarly $\langle \varepsilon,\ m\rangle \in r^n$ implies $m = \varepsilon$. It follows that $m = \varepsilon \in \{\varepsilon\} \triangleq B[\![\varepsilon]\!]r$.

— Second, we show that

$$m' \in \mathbb{A}[\![RS]\!] \wedge \langle m',\ m\rangle \in r^n \Rightarrow m \in B[\![RS]\!]r^n \tag{17}$$

The proof is by structural induction on RS.

- The base case $RS = S$ follows from the previous lemma (17) since $\mathbb{A}[\![S]\!] = \{\mathbb{R}[\![S]\!]\}$;
- Otherwise $RS = SRS'$. If $m' \in \mathbb{A}[\![SRS']\!]$ then $m' \in \mathbb{A}[\![S]\!] \cdot \mathbb{A}[\![RS']\!]$ by (2) so $m' = s'q'$ where $s' \in \mathbb{A}[\![S]\!]$ and $q' \in \mathbb{A}[\![RS']\!]$.

  Since $\langle m',\, m\rangle = \langle s'q',\, m\rangle \in r^n$ the separate derivation corollary **4** implies that $m = pq$ with $\langle s',\, p\rangle \in r^n$ and $\langle q',\, q\rangle \in r^n$.

  So by the previous lemma (17), $p \in B[\![S]\!]r^n$ and by ind. hyp., $q \in B[\![RS']\!]r^n$.

  By def. (4) of $B[\![SRS']\!]$, we have $m = pq \in B[\![S]\!]r^n \cdot B[\![RS']\!]r^n = B[\![RS]\!]r^n$.

— Third, we show that

$$m' \in \mathbb{A}[\![ARS]\!] \wedge \langle m',\, m\rangle \in r^n \Rightarrow m \in B[\![ARS]\!]r^n \tag{18}$$

The proof is by structural induction on ARS:

- The base case $ARS = RS$ is handled by the previous lemma (18);
- Otherwise $ARS = RS \mid ARS'$ so if $m' \in \mathbb{A}[\![RS \mid ARS']\!] = \mathbb{A}[\![RS]\!] \cup \mathbb{A}[\![ARS']\!]$ by (2) then two cases have to be considered:
  - Either $m' \in \mathbb{A}[\![ARS']\!]$ so $\langle m',\, m\rangle \in r^n$ implies $m \in B[\![ARS']\!]r^n$ by induction hypothesis;
  - Otherwise $m' \in \mathbb{A}[\![RS]\!]$ so $\langle m',\, m\rangle \in r^n$ implies $m \in B[\![RS]\!]r^n$ by the previous lemma (18).

  It follows that $m \in B[\![RS]\!]r^n \cup B[\![ARS']\!]r^n = B[\![RS \mid ARS']\!]r^n = B[\![ARS]\!]r^n$ by (3).

— Fourth, we show that

$$\text{if } P = N ::= ARS \quad \text{then} \quad \tau[\![P]\!] \circ r^n \subseteq B[\![P]\!]r^n \tag{19}$$

Let us calculate

$$\begin{aligned}
& \tau[\![P]\!] \circ r^n \\
= \ & \{\langle pNq,\, pm'q\rangle \mid p, q \in \mathbb{V}[\![G]\!]^\star \wedge m' \in \mathbb{A}[\![ARS]\!]\} \circ r^n \quad \wr\text{by def. (2) of } \tau[\![P]\!]\wr \\
= \ & \{\langle pNq,\, s\rangle \mid p, q \in \mathbb{V}[\![G]\!]^\star \wedge m' \in \mathbb{A}[\![ARS]\!] \wedge \langle pm'q,\, s\rangle \in r^n\} \quad \wr\text{by def. } \circ\wr \\
\subseteq \ & \{\langle pNq,\, p'mq'\rangle \mid p, q, p', q' \in \mathbb{V}[\![G]\!]^\star \wedge m' \in \mathbb{A}[\![ARS]\!] \wedge \langle p,\, p'\rangle \in r^n \wedge \langle m',\\
& m\rangle \in r^n \wedge \langle q,\, q'\rangle \in r^n\} \quad \wr\text{by the separate derivation corollary } \mathbf{4}\wr
\end{aligned}$$

$\subseteq$ $\{\langle pNq,\ p'mq'\rangle \mid p, q, p', q' \in \mathbb{V}[\![G]\!]^\star \wedge \langle p,\ p'\rangle \in r^n \wedge m \in B[\![ARS]\!]r^n \wedge \langle q,\ q'\rangle \in r^n\}$ $\wr$ by the previous lemma (19)$\int$

$\subseteq$ $B[\![P]\!]r^n$ $\wr$by $P = N ::= ARS$ and def. (9) of $B[\![P]\!]$$\int$

— Fifth, we show that

$$\tau[\![G]\!] \circ r^n \quad \subseteq \quad B[\![G]\!]r^n \tag{20}$$

The proof is by structural induction on G.

– The base case $G = P$ follows from the previous lemma (20).

– Otherwise $G = PG'$, and then

$$\begin{aligned}
& \tau[\![PG']\!] \circ r^n \\
= \ & (\tau[\![P]\!] \cup \tau[\![G']\!]) \circ r^n && \wr\text{by def. (2) of } \tau[\![PG']\!]\int \\
= \ & (\tau[\![P]\!] \circ r^n) \cup (\tau[\![G']\!] \circ r^n) && \wr\text{by def. } \circ\int \\
\subseteq \ & B[\![P]\!]r^n \cup B[\![G']\!]r^n && \wr\text{by previous lemma (20) and ind. hyp.}\int \\
= \ & B[\![G]\!]r^n && \wr\text{by } G = PG' \text{ and def. (8) of } B[\![G]\!]\int
\end{aligned}$$

— Sixth, we show that

$$B[\![G]\!]r^n \quad \subseteq \quad S^d[\![G]\!] \quad \triangleq \quad \mathbf{lfp}_{\emptyset}^{\subseteq} B[\![G]\!] \tag{21}$$

The proof is by recurrence on n.

– For $n = 0$, we have $G = P$ or $G = PG'$ so by (8) and (9), $\tau[\![G]\!]^0 = \mathsf{I}_{\mathbb{V}^\star} \subseteq B[\![G]\!](S^d[\![G]\!]) = S^d[\![G]\!]$ by the fixpoint property $S^d[\![G]\!] \triangleq \mathbf{lfp}^{\subseteq} B[\![G]\!]$;

– For $n + 1$, we have $r^{n+1} = \bigcup_{k=0}^{n+1} \tau[\![G]\!]^k = \tau[\![G]\!]^0 \cup \bigcup_{k=0}^{n} \tau[\![G]\!]^{k+1} = \mathsf{I}_{\mathbb{V}^\star} \cup \tau[\![G]\!] \circ \bigcup_{k=0}^{n} \tau[\![G]\!]^k = \mathsf{I}_{\mathbb{V}^\star} \cup \tau[\![G]\!] \circ r^n$.

  We have just shown above that $\mathsf{I}_{\mathbb{V}^\star} \subseteq S^d[\![G]\!]$. It remains to prove that $\tau[\![G]\!] \circ r^n \subseteq S^d[\![G]\!]$.

  We have $\tau[\![G]\!] \circ r^n \subseteq B[\![G]\!]r^n$ by the previous lemma (21) and $B[\![G]\!]r^n \subseteq S^d[\![G]\!]$ by recurrence hypothesis so $\tau[\![G]\!] \circ r^n \subseteq S^d[\![G]\!]$ by transitivity. ∎

— Seventh and finally,

$$
\begin{aligned}
& \tau[\![G]\!]^{\star} \\
= \;& \mathsf{I}_{\mathbb{V}^{\star}} \cup \tau[\![G]\!] \circ \tau[\![G]\!]^{\star} && \wr \text{fixpoint definition of } \tau[\![G]\!]^{\star} \text{ in question 7} \int \\
= \;& \mathsf{I}_{\mathbb{V}^{\star}} \cup \tau[\![G]\!] \circ \bigcup_{n \geq 0} r^{n} && \wr\, \tau[\![G]\!]^{\star} = \bigcup_{n \geq 0} r^{n} \int \\
= \;& \mathsf{I}_{\mathbb{V}^{\star}} \cup \bigcup_{n \geq 0} \tau[\![G]\!] \circ r^{n} && \wr \text{by def. } \circ \int \\
\subseteq \;& \mathsf{I}_{\mathbb{V}^{\star}} \cup \bigcup_{n \geq 0} B[\![G]\!] r^{n} && \wr \text{by previous lemma (21)} \int \\
\subseteq \;& S^{d}[\![G]\!] && \wr \text{by previous lemma (22)} \int \quad \blacksquare
\end{aligned}
$$