Lemma und.1. Verifying the Representation

In order to verify that our representation works, we have to prove two things. First, we have to show that if \( M \) halts on input \( w \), then \( \tau(M, w) \rightarrow a(M, w) \) is valid. Then, we have to show the converse, i.e., that if \( \tau(M, w) \rightarrow a(M, w) \) is valid, then \( M \) does in fact eventually halt when run on input \( w \).

The strategy for proving these is very different. For the first result, we have to show that a sentence of first-order logic (namely, \( \tau(M, w) \rightarrow a(M, w) \)) is valid. The easiest way to do this is to give a derivation. Our proof is supposed to work for all \( M \) and \( w \), though, so there isn’t really a single sentence for which we have to give a derivation, but infinitely many. So the best we can do is to prove by induction that, whatever \( M \) and \( w \) look like, and however many steps it takes \( M \) to halt on input \( w \), there will be a derivation of \( \tau(M, w) \rightarrow a(M, w) \).

Naturally, our induction will proceed on the number of steps \( M \) takes before it reaches a halting configuration. In our inductive proof, we’ll establish that for each step \( n \) of the run of \( M \) on input \( w \), \( \tau(M, w) \models \chi(M, w, n) \), where \( \chi(M, w, n) \) correctly describes the configuration of \( M \) run on \( w \) after \( n \) steps. Now if \( M \) halts on input \( w \) after, say, \( n \) steps, \( \chi(M, w, n) \) will describe a halting configuration. We’ll also show that \( \chi(M, w, n) \models a(M, w) \), whenever \( \chi(M, w, n) \) describes a halting configuration. So, if \( M \) halts on input \( w \), then for some \( n \), \( M \) will be in a halting configuration after \( n \) steps. Hence, \( \tau(M, w) \models \chi(M, w, n) \models a(M, w) \), where \( \chi(M, w, n) \) describes a halting configuration, and since in that case \( \chi(M, w, n) \models a(M, w) \), we get that \( T(M, w) \models a(M, w) \), i.e., that \( \models \tau(M, w) \rightarrow a(M, w) \).

The strategy for the converse is very different. Here we assume that \( \models \tau(M, w) \rightarrow a(M, w) \) and have to prove that \( M \) halts on input \( w \). From the hypothesis we get that \( \tau(M, w) \models a(M, w) \), i.e., \( a(M, w) \) is true in every structure in which \( \tau(M, w) \) is true: its domain will be \( \mathbb{N} \), and the interpretation of all the \( Q_q \) and \( S_x \) will be given by the configurations of \( M \) during a run on input \( w \). So, e.g., \( \mathfrak{M} \models Q_q(\overline{m}, \overline{q}) \) iff \( T \), when run on input \( w \) for \( n \) steps, is in state \( q \) and scanning square \( m \). Now since \( \tau(M, w) \models a(M, w) \) by hypothesis, and since \( \mathfrak{M} \models \tau(M, w) \) by construction, \( \mathfrak{M} \models a(M, w) \). But \( \mathfrak{M} \models a(M, w) \) iff there is some \( n \in |\mathfrak{M}| = \mathbb{N} \) so that \( M \), run on input \( w \), is in a halting configuration after \( n \) steps.

Definition und.1. Let \( \chi(M, w, n) \) be the sentence

\[
Q_q(\overline{m}, \overline{q}) \land S_{\sigma_0}(\overline{0}, \overline{q}) \land \cdots \land S_{\sigma_k}(\overline{k}, \overline{q}) \land \forall x (\overline{k} < x \rightarrow S_{\sigma_k}(x, \overline{q}))
\]

where \( q \) is the state of \( M \) at time \( n \), \( M \) is scanning square \( m \) at time \( n \), square \( i \) contains symbol \( \sigma_i \) at time \( n \) for \( 0 \leq i \leq k \) and \( k \) is the right-most non-blank square of the tape at time 0, or the right-most square the tape head has visited after \( n \) steps, whichever is greater.

Lemma und.2. If \( M \) run on input \( w \) is in a halting configuration after \( n \) steps, then \( \chi(M, w, n) \models a(M, w) \).

verification rev: 788b9aa (2022-03-22) by OLP / CC–BY
Proof. Suppose that $M$ halts for input $w$ after $n$ steps. There is some state $q$, square $m$, and symbol $\sigma$ such that:

1. After $n$ steps, $M$ is in state $q$ scanning square $m$ on which $\sigma$ appears.
2. The transition function $\delta(q, \sigma)$ is undefined.

$\chi(M, w, n)$ is the description of this configuration and will include the clauses $Q_q(m, n)$ and $S_\sigma(m, n)$. These clauses together imply $\alpha(M, w)$:

$$\exists x \exists y \left( \bigvee_{(q, \sigma) \in X} (Q_q(x, y) \land S_\sigma(x, y)) \right)$$

since $Q_{q'}(m, n) \land S_{\sigma'}(m, n) \models \bigvee_{(q, \sigma) \in X} (Q_q(m, n) \land S_\sigma(m, n))$, as $\langle q', \sigma' \rangle \in X$. $\square$

So if $M$ halts for input $w$, then there is some $n$ such that $\chi(M, w, n) \models \alpha(M, w)$. We will now show that for any time $n$, $\tau(M, w) \models \chi(M, w, n)$.

Lemma 3. For each $n$, if $M$ has not halted after $n$ steps, $\tau(M, w) \models \chi(M, w, n)$.

Proof. Induction basis: If $n = 0$, then the conjuncts of $\chi(M, w, 0)$ are also conjuncts of $\tau(M, w)$, so entailed by it.

Inductive hypothesis: If $M$ has not halted before the $n$th step, then $\tau(M, w) \models \chi(M, w, n)$. We have to show that (unless $\chi(M, w, n)$ describes a halting configuration), $\tau(M, w) \models \chi(M, w, n+1)$.

Suppose $n > 0$ and after $n$ steps, $M$ started on $w$ is in state $q$ scanning square $m$. Since $M$ does not halt after $n$ steps, there must be an instruction of one of the following three forms in the program of $M$:

1. $\delta(q, \sigma) = \langle q', \sigma', R \rangle$
2. $\delta(q, \sigma) = \langle q', \sigma', L \rangle$
3. $\delta(q, \sigma) = \langle q', \sigma', N \rangle$

We will consider each of these three cases in turn.

1. Suppose there is an instruction of the form (1). By ????, this means that

$$\forall x \forall y ((Q_q(x, y) \land S_\sigma(x, y)) \rightarrow (Q_{q'}(x', y') \land S_{\sigma'}(x', y') \land \varphi(x, y)))$$

is a conjunct of $\tau(M, w)$. This entails the following sentence (universal instantiation, $m$ for $x$ and $\pi$ for $y$):

$$(Q_q(m, \pi) \land S_\sigma(m, \pi)) \rightarrow (Q_{q'}(m', \pi') \land S_{\sigma'}(m, \pi) \land \varphi(m, \pi)).$$
By induction hypothesis, \( \tau(M, w) \models \chi(M, w, n) \), i.e.,

\[
Q_q(m, n) \land S_{\sigma_0}(\overline{0}, n) \land \cdots \land S_{\sigma_k}(\overline{k}, n) \land \\
\forall x (\overline{k} < x \rightarrow S_0(x, n))
\]

Since after \( n \) steps, tape square \( m \) contains \( \sigma \), the corresponding conjunct is \( S_{\sigma}(m, n) \), so this entails:

\[
Q_q(m, n) \land S_{\sigma}(m, n)
\]

We now get

\[
Q_{q'}(m', n') \land S_{\sigma'}(m', n') \land \\
S_{\sigma_0}(\overline{0}, n') \land \cdots \land S_{\sigma_k}(\overline{k}, n') \land \\
\forall x (\overline{k} < x \rightarrow S_0(x, n'))
\]

as follows: The first line comes directly from the consequent of the preceding conditional, by modus ponens. Each conjunct in the middle line—which excludes \( S_{\sigma_m}(m, n') \)—follows from the corresponding conjunct in \( \chi(M, w, n) \) together with \( \varphi(m, n) \).

If \( m < k \), \( \tau(M, w) \vdash m < k \) (??) and by transitivity of \( < \), we have \( \forall x (\overline{k} < x \rightarrow m < x) \). If \( m = k \), then \( \forall x (\overline{k} < x \rightarrow m < x) \) by logic alone. The last line then follows from the corresponding conjunct in \( \chi(M, w, n) \), \( \forall x (\overline{k} < x \rightarrow m < x) \), and \( \varphi(m, n) \). If \( m < k \), this already is \( \chi(M, w, n+1) \).

Now suppose \( m = k \). In that case, after \( n + 1 \) steps, the tape head has also visited square \( k + 1 \), which now is the right-most square visited. So \( \chi(M, w, n + 1) \) has a new conjunct, \( S_0(\overline{k}, n') \), and the last conjuct is \( \forall x (\overline{k} < x \rightarrow S_0(x, n')) \). We have to verify that these two sentences are also implied.

We already have \( \forall x (\overline{k} < x \rightarrow S_0(x, n')) \). In particular, this gives us \( \overline{k} < \overline{k}' \rightarrow S_0(\overline{k}, n') \). From the axiom \( \forall x x < x' \) we get \( \overline{k} < \overline{k}' \). By modus ponens, \( S_0(\overline{k'}, n') \) follows.

Also, since \( \tau(M, w) \vdash \overline{k} < \overline{k}' \), the axiom for transitivity of \( < \) gives us \( \forall x (\overline{k'} < x \rightarrow S_0(x, n')) \). (We leave the verification of this as an exercise.)

2. Suppose there is an instruction of the form (2). Then, by ???,

\[
\forall x \forall y ((Q_q(x', y) \land S_{\sigma}(x', y)) \rightarrow \\
(Q_{q'}(x', y') \land S_{\sigma'}(x', y') \land \varphi(x, y))) \land \\
\forall y ((Q_q(0, y) \land S_{\sigma}(0, y)) \rightarrow \\
(Q_{q'}(0, y') \land S_{\sigma'}(0, y') \land \varphi(0, y)))
\]
is a conjunct of $\tau(M, w)$. If $m > 0$, then let $l = m - 1$ (i.e., $m = l + 1$).
The first conjunct of the above sentence entails the following:

$$(Q_q(l, \pi) \land S_\sigma(l, \pi)) \rightarrow (Q_{q'}(l', \pi') \land S_\sigma(l', \pi' \land \varphi(l, \pi)))$$

Otherwise, let $l = m = 0$ and consider the following sentence entailed by
the second conjunct:

$$((Q_{q_i}(0, \pi) \land S_\sigma(0, \pi)) \rightarrow (Q_{q_j}(0, \pi') \land S_\sigma(0, \pi') \land \varphi(0, \pi)))$$

Either sentence implies

$$Q_{q'}(l, \pi') \land S_\sigma(l, \pi') \land S_\sigma(0, \pi') \land \forall x (k < x \rightarrow S_0(x, \pi'))$$

as before. (Note that in the first case, $l' \equiv l + 1 \equiv m$ and in the second
case $l \equiv 0$.) But this just is $\chi(M, w, n + 1)$.

3. Case (3) is left as an exercise.

We have shown that for any $n$, $\tau(M, w) \models \chi(M, w, n)$.

**Problem und.1.** Complete case (3) of the proof of Lemma und.3.

**Problem und.2.** Give a derivation of $S_\sigma(i, \pi')$ from $S_\sigma(i, \pi)$ and $\varphi(m, n)$
(assuming $i \neq m$, i.e., either $i < m$ or $m < i$).

**Problem und.3.** Give a derivation of $\forall x (k < x \rightarrow S_0(x, \pi'))$ from $\forall x (k < x \rightarrow S_0(x, \pi'))$, $\forall x < x'$, and $\forall x \forall y \forall z ((x < y \land y < z) \rightarrow x < z)$.

**Lemma und.4.** If $M$ halts on input $w$, then $\tau(M, w) \rightarrow \alpha(M, w)$ is valid.

**Proof.** By Lemma und.3, we know that, for any time $n$, the description $\chi(M, w, n)$
of the configuration of $M$ at time $n$ is entailed by $\tau(M, w)$. Suppose $M$ halts
after $k$ steps. At that point, it will be scanning square $m$, for some $m \in \mathbb{N}$. Then
$\chi(M, w, k)$ describes a halting configuration of $M$, i.e., it contains as conjuncts
both $Q_q(m, \overline{E})$ and $S_\sigma(m, \overline{E})$ with $\delta(q, \sigma)$ undefined. Thus, by Lemma und.2,
$\chi(M, w, k) \models \alpha(M, w)$. But since $\tau(M, w) \models \chi(M, w, k)$, we have $\tau(M, w) \models \alpha(M, w)$ and therefore $\tau(M, w) \rightarrow \alpha(M, w)$ is valid.

To complete the verification of our claim, we also have to establish the reverse direction: if $\tau(M, w) \rightarrow \alpha(M, w)$ is valid, then $M$ does in fact halt when
started on input $w$. 

explanation

verification rev: 788b9aa (2022-03-22) by OLP / CC–BY
Lemma und. 5. If $\models \tau(M, w) \rightarrow \alpha(M, w)$, then $M$ halts on input $w$.

Proof. Consider the $\mathcal{L}_M$-structure $\mathfrak{M}$ with domain $\mathbb{N}$ which interprets $0$ as $0$, $\mathcal{I}$ as the successor function, and $\prec$ as the less-than relation, and the predicates $Q_q$ and $S_\sigma$ as follows:

- $Q_q^m = \{ (m, n) : \text{started on } w, \text{after } n \text{ steps, } M \text{ is in state } q \text{ scanning square } m \}$
- $S_\sigma^m = \{ (m, n) : \text{started on } w, \text{after } n \text{ steps, square } m \text{ of } M \text{ contains symbol } \sigma \}$

In other words, we construct the structure $\mathfrak{M}$ so that it describes what $M$ started on input $w$ actually does, step by step. Clearly, $\mathfrak{M} \models \tau(M, w)$. If $\models \tau(M, w) \rightarrow \alpha(M, w)$, then also $\mathfrak{M} \models \alpha(M, w)$, i.e.,

$$\mathfrak{M} \models \exists x \exists y \left( (Q_q(x, y) \land S_\sigma(x, y)) \right).$$

As $|\mathfrak{M}| = \mathbb{N}$, there must be $m, n \in \mathbb{N}$ so that $\mathfrak{M} \models Q_q(m, n) \land S_\sigma(m, n)$ for some $q$ and $\sigma$ such that $\delta(q, \sigma)$ is undefined. By the definition of $\mathfrak{M}$, this means that $M$ started on input $w$ after $n$ steps is in state $q$ and reading symbol $\sigma$, and the transition function is undefined, i.e., $M$ has halted.

Photo Credits

Bibliography