und.1 Verifying the Representation

tur:und:ver: sec

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 $\tau(M, w) \to \alpha(M, w)$ is valid. Then, we have to show the converse, i.e., that if $\tau(M, w) \to \alpha(M, w)$ is valid, then M does in fact eventually halt when run on input w. explanation

The strategy for proving these is very different. For the first result, we have to show that a sentence of first-order logic (namely, $\tau(M, w) \to \alpha(M, w)$) 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 $\tau(M, w) \to \alpha(M, w)$.

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, $\tau(M, w) \vDash \chi(M, w, n)$, 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 $\chi(M, w, n) \vDash \alpha(M, w)$, 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, $\tau(M, w) \vDash \chi(M, w, n)$ where $\chi(M, w, n)$ describes a halting configuration, and since in that case $\chi(M, w, n) \vDash \alpha(M, w)$, we get that $T(M, w) \vDash \alpha(M, w)$, i.e., that $\vDash \tau(M, w) \to \alpha(M, w)$.

The strategy for the converse is very different. Here we assume that $\vDash \tau(M, w) \to \alpha(M, w)$ and have to prove that M halts on input w. From the hypothesis we get that $\tau(M, w) \vDash \alpha(M, w)$, i.e., $\alpha(M, w)$ is true in every structure in which $\tau(M, w)$ is true. So we'll describe a structure $\mathfrak{M}$ in which $\tau(M, w)$ is true: its domain will be $\mathbb{N}$, and the interpretation of all the Q_q and S_σ will be given by the configurations of M during a run on input w. So, e.g., $\mathfrak{M} \vDash Q_q(\overline{m}, \overline{n})$ iff T, when run on input w for n steps, is in state q and scanning square m. Now since $\tau(M, w) \vDash \alpha(M, w)$ by hypothesis, and since $\mathfrak{M} \vDash \tau(M, w)$ by construction, $\mathfrak{M} \vDash \alpha(M, w)$. But $\mathfrak{M} \vDash \alpha(M, w)$ 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

$$Q_q(\overline{m}, \overline{n}) \land S_{\sigma_0}(\overline{0}, \overline{n}) \land \dots \land S_{\sigma_k}(\overline{k}, \overline{n}) \land \forall x\, (\overline{k} < x \to S_0(x, \overline{n}))$$

where q is the state of M at time n, M is scanning square m at time n, square i contains symbol σ_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.

tur:und:ver: lem:halt-config-implies-halt

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

Proof. Suppose that M halts for input w after n steps. There is some state q, square m, and symbol σ such that:

1. After n steps, M is in state q scanning square m on which σ 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 $Q_q(\overline{m}, \overline{n})$ and $S_\sigma(\overline{m}, \overline{n})$. These clauses together imply $\alpha(M, w)$:

$$\exists x\, \exists y\, \Big(\bigvee_{\langle q,\sigma\rangle \in X} (Q_q(x, y) \land S_\sigma(x, y))\Big)$$

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

explanation

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

Lemma und.3. *For each n, if M has not halted after n steps, $\tau(M, w) \vDash \chi(M, w, n)$.* *tur:und:ver:lem:config*

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 nth step, then $\tau(M, w) \vDash \chi(M, w, n)$. We have to show that (unless $\chi(M, w, n)$ describes a halting configuration), $\tau(M, w) \vDash \chi(M, w, n + 1)$.

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. $\delta(q, \sigma) = \langle q', \sigma', R\rangle$ tur:und:ver:right
2. $\delta(q, \sigma) = \langle q', \sigma', L\rangle$ tur:und:ver:left
3. $\delta(q, \sigma) = \langle q', \sigma', N\rangle$ tur:und:ver:stay

We will consider each of these three cases in turn.

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

$$\begin{aligned}\forall x\, \forall y\, ((&Q_q(x, y) \land S_\sigma(x, y)) \to\\ &(Q_{q'}(x', y') \land S_{\sigma'}(x, y') \land \varphi(x, y)))\end{aligned}$$

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

$$\begin{aligned}(&Q_q(\overline{m}, \overline{n}) \land S_\sigma(\overline{m}, \overline{n})) \to\\ &(Q_{q'}(\overline{m}', \overline{n}') \land S_{\sigma'}(\overline{m}, \overline{n}') \land \varphi(\overline{m}, \overline{n})).\end{aligned}$$

 verification rev: 016d2bc (2024-06-22) by OLP / CC–BY

By induction hypothesis, $\tau(M, w) \vDash \chi(M, w, n)$, i.e.,

$$\begin{aligned} & Q_q(\overline{m}, \overline{n}) \land S_{\sigma_0}(\overline{0}, \overline{n}) \land \dots \land S_{\sigma_k}(\overline{k}, \overline{n}) \land \\ & \quad \forall x\, (\overline{k} < x \to S_0(x, \overline{n})) \end{aligned}$$

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

$$Q_q(\overline{m}, \overline{n}) \land S_\sigma(\overline{m}, \overline{n})$$

We now get

$$\begin{aligned} & Q_{q'}(\overline{m}', \overline{n}') \land S_{\sigma'}(\overline{m}, \overline{n}') \land \\ & \quad S_{\sigma_0}(\overline{0}, \overline{n}') \land \dots \land S_{\sigma_k}(\overline{k}, \overline{n}') \land \\ & \quad \forall x\, (\overline{k} < x \to S_0(x, \overline{n}')) \end{aligned}$$

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 $S_{\sigma_m}(\overline{m}, \overline{n}')$—follows from the corresponding conjunct in $\chi(M, w, n)$ together with $\varphi(\overline{m}, \overline{n})$.

If $m < k$, $\tau(M, w) \vdash \overline{m} < \overline{k}$ (**??**) and by transitivity of $<$, we have $\forall x\, (\overline{k} < x \to \overline{m} < x)$. If $m = k$, then $\forall x\, (\overline{k} < x \to \overline{m} < x)$ by logic alone. The last line then follows from the corresponding conjunct in $\chi(M, w, n)$, $\forall x\, (\overline{k} < x \to \overline{m} < x)$, and $\varphi(\overline{m}, \overline{n})$. 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, $S_0(\overline{k}', \overline{n}')$, and the last conjunct is $\forall x\, (\overline{k}' < x \to S_0(x, \overline{n}'))$. We have to verify that these two sentences are also implied.

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

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

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

$$\begin{aligned} & \forall x\, \forall y\, ((Q_q(x', y) \land S_\sigma(x', y)) \to \\ & \quad (Q_{q'}(x, y') \land S_{\sigma'}(x', y') \land \varphi(x, y))) \land \\ & \forall y\, ((Q_{q_i}(\overline{0}, y) \land S_\sigma(\overline{0}, y)) \to \\ & \quad (Q_{q_j}(\overline{0}, y') \land S_{\sigma'}(\overline{0}, y') \land \varphi(\overline{0}, y))) \end{aligned}$$

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:

$$(Q_q(\overline{l}', \overline{n}) \land S_\sigma(\overline{l}', \overline{n})) \to$$
$$(Q_{q'}(\overline{l}, \overline{n}') \land S_{\sigma'}(\overline{l}', \overline{n}') \land \varphi(\overline{l}, \overline{n}))$$

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

$$((Q_{q_i}(\overline{0}, \overline{n}) \land S_\sigma(\overline{0}, \overline{n})) \to$$
$$(Q_{q_j}(\overline{0}, \overline{n}') \land S_{\sigma'}(\overline{0}, \overline{n}') \land \varphi(\overline{0}, \overline{n})))$$

Either sentence implies

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

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

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

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

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

Problem und.2. Give a derivation of $S_{\sigma_i}(\overline{i}, \overline{n}')$ from $S_{\sigma_i}(\overline{i}, \overline{n})$ and $\varphi(m, n)$ (assuming $i \neq m$, i.e., either $i < m$ or $m < i$).

Problem und.3. Give a derivation of $\forall x\, (\overline{k}' < x \to S_0(x, \overline{n}'))$ from $\forall x\, (\overline{k} < x \to S_0(x, \overline{n}'))$, $\forall x\, x < x'$, and $\forall x\, \forall y\, \forall z\, ((x < y \land y < z) \to x < z)$.)

Lemma und.4. *If M halts on input w, then $\tau(M, w) \to \alpha(M, w)$ is valid.* *tur:und:ver: lem:valid-if-halt*

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 $Q_q(\overline{m}, \overline{k})$ and $S_\sigma(\overline{m}, \overline{k})$ with $\delta(q, \sigma)$ undefined. Thus, by Lemma und.2, $\chi(M, w, k) \vDash \alpha(M, w)$. But since $\tau(M, w) \vDash \chi(M, w, k)$, we have $\tau(M, w) \vDash \alpha(M, w)$ and therefore $\tau(M, w) \to \alpha(M, w)$ is valid. □

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

tur:und:ver: lem:halt-if-valid **Lemma und.5.** *If* $\vDash \tau(M, w) \to \alpha(M, w)$*, then* M *halts on input* w*.*

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

$$Q_q^{\mathfrak{M}} = \{\langle m, n\rangle : \begin{array}{l}\text{started on } w\text{, after } n \text{ steps,}\\ M \text{ is in state } q \text{ scanning square } m\end{array}\}$$

$$S_\sigma^{\mathfrak{M}} = \{\langle m, n\rangle : \begin{array}{l}\text{started on } w\text{, after } n \text{ steps,}\\ \text{square } m \text{ of } M \text{ contains symbol } \sigma\end{array}\}$$

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, $\mathfrak{M} \vDash \tau(M, w)$. If $\vDash \tau(M, w) \to \alpha(M, w)$, then also $\mathfrak{M} \vDash \alpha(M, w)$, i.e.,

$$\mathfrak{M} \vDash \exists x\, \exists y\, (\bigvee_{\langle q,\sigma\rangle \in X} (Q_q(x, y) \land S_\sigma(x, y))).$$

As $|\mathfrak{M}| = \mathbb{N}$, there must be m, $n \in \mathbb{N}$ so that $\mathfrak{M} \vDash Q_q(\overline{m}, \overline{n}) \land S_\sigma(\overline{m}, \overline{n})$ for some q and σ 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 σ, and the transition function is undefined, i.e., M has halted. □

Photo Credits

Bibliography